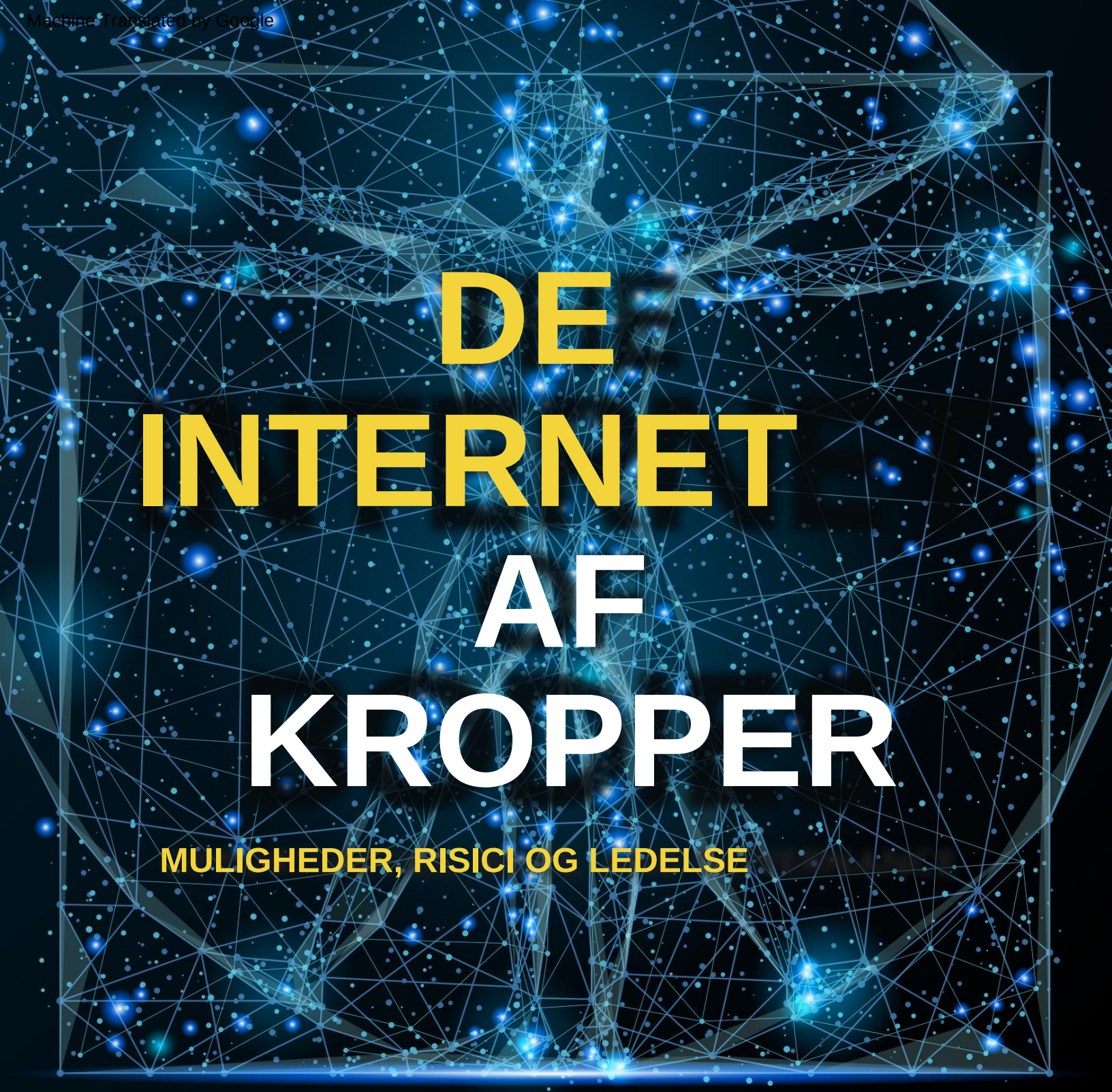
Machine Translated by Google



DE INTERNET AF KROPPER

MULIGHEDER, RISICI OG LEDELSE

MARY LEE | BENJAMIN BOUDREAUX | RITIKA CHATURVEDI
SASHA ROMANOSKY | BRYCE DOWNING

RAND CORPORATION

Machine Translated by Google

Omslagsdesign: Peter Soriano
Forsidebillede: Adobe Stock/ anttoniart.

Begrænsede rettigheder til trykte og elektroniske distributionsrettigheder

Dette dokument og de heri indeholdte varemærker er beskyttet af loven. Denne repræsentation af RANDs intellektuelle ejendom er kun til ikke-kommerciel brug. Uautoriseret offentliggørelse af denne publikation online er forbudt. Der gives tilladelse til at duplikere dette dokument kun til personlig brug, så længe det er uændret og fuldstændigt. RAND kræver tilladelse til at reproducere eller genbruge i en anden form vores forskningsdokumenter til kommerciel brug. For information om genoptryk og linktilladelser, besøg venligst www.rand.org/pubs/permissions.html.

RANDs publikationer afspejler ikke nødvendigvis meningerne hos deres forskningsklienter og sponsorer. R® er et registreret varemærke.

For mere information om denne publikation, besøg
www.rand.org/t/RR3226

Library of Congress' katalogiseringsdata for publikationer er tilgængelige for denne publikation.

ISBN: 978-1-9774-0522-7

© Ophavsret 2020 RAND Corporation

Machine Translated by Google

Hvad er kroppenes internet?

Et bredt udvalg af internetforbundne "smarte" enheder lover nu forbrugere og virksomheder forbedret ydeevne, bekvemmelighed, effektivitet og sjov. Inden for dette

Det bredere Internet of Things (IoT) ligger i en voksende industri af enheder, der overvåger menneskekroppen, indsamler sundheds- og andre personlige oplysninger og overfører disse data via internettet. Vi omtaler disse nye teknologier og de data, de indsamler, som Internet of Bodies (IoB) (se f.eks. Neal, 2014; Lee, 2018), et udtryk, der først blev anvendt om lov og politik i 2016 af jura- og ingeniørprofessor Andrea M.
Matwyshyn (Atlantiske Råd, 2017; Matwyshyn, 2016; Matwyshyn, 2018; Matawyshyn, 2019).

IoB-enheder findes i mange former. Nogle er allerede i vid udstrækning anvendt, såsom armbåndsure til fitnessmonitorer eller pacemakere, der sender data om en patients hjerte direkte til en kardiolog. Andre produkter, der er under udvikling eller nyligt er kommet på markedet, er måske mindre velkendte, såsom indtagelige produkter, der indsamler og sender information om en persons tarm, mikrochipimplantater, hjernestimuleringsenheder og internetforbundne toiletter.

Disse enheder har intim adgang til kroppen og indsamler enorme mængder af personlige biometriske data. Producenter af IoB-enheder lover at levere betydelige sundhedsmæssige og andre fordele, men udgør også alvorlige risici, herunder risiko for hacking, krænkelser af privatlivets fred eller funktionsfejl. Nogle enheder, såsom en pålidelig kunstig bugspytkirtel til diabetikere, kan revolutionere behandlingen af sygdomme, mens andre blot kan oppuste sundhedsomkostningerne med ringe positiv effekt på resultaterne. Adgang til enorme strømme af livestreaming af biometriske data kan udløse gennembrud inden for medicinsk viden eller adfærdsforståelse. Det kan øge ulighederne i sundhedsresultater, hvor kun mennesker med økonomiske midler har adgang til nogen af disse fordele. Eller det kan muliggøre en overvågningstilstand med hidtil uset indtrængen og konsekvenser.

Der findes ingen universelt accepteret definition af IoB.1 I denne rapport refererer vi til IoB, eller IoB-økosystemet, som IoB-enheder (defineret nedenfor, med yderligere forklaring i de følgende passager) sammen med den software, de indeholder, og de data, de indsamler.2

Forkortelser

AI	kunstig intelligens
CCPA	Californiens forbrugerbeskyttelseslov
CFIUS	Udvalget for Udenlandske Investeringer i USA
CGM	kontinuerlig glukosemåler
CPAP	kontinuerligt positivt luftvejstryk
EHR	elektronisk patientjournal
EU	Den Europæiske Union
Slutbrugerlicensaftale	slutbrugerlicensaftale
FDA	Den amerikanske fødevare- og lægemiddelstyrelse
FTC	Den føderale handelskommission
GDPR	Generel databeskyttelse Regulering
H-ISAC	Deling af sundhedsoplysninger Analysecenter
HIPAA	Portabilitet af sundhedsforsikring og Ansvarlighedsloven
ICS-CERT	Industrielle Styresystemer Cyber Beredskabsteam
IoB	Kroppernes internet
IoT	Tingenes Internet
MDIC	Innovation inden for medicinsk udstyr Konsortium
[illegible]	ikke-smitsom sygdom
NFC	nærfeltskommunikation
NIST	Nationalt Institut for Standarder og Teknologi
NITRD	Netværk og information Teknologiforskning og Udvikling
PGHD	persongenererede sundhedsdata
RFID	radiofrekvensidentifikation

Machine Translated by Google

En IoB-enhed er defineret som en enhed, der

- indeholder software eller computerfunktioner
- kan kommunikere med en internetforbundet enhed eller et netværk

og opfylder et eller begge af følgende:

- indsamler persongenererede sundheds- eller biometriske oplysninger data
- kan ændre menneskekroppens funktion.

Softwaren eller computerfunktionerne i en IoB-enhed kan være så simple som et par linjer kode, der bruges til at konfigurere et RFID-mikrochipimplantat (radiofrekvensidentifikation), eller så komplekse som en computer, der behandler kunstig intelligens (AI) og maskinlæringsalgoritmer. En internetforbindelse via mobil- eller Wi-Fi-netværk er påkrævet, men behøver ikke at være en direkte forbindelse. For eksempel kan en enhed være tilsluttet via Bluetooth til en smartphone eller USB-enhed, der kommunikerer med en internetforbundet computer.
Persongenererede sundhedsdata (PGHD) refererer til sundheds-, kliniske eller velværedata indsamlet af teknologier, der skal registreres eller analyseres af brugeren eller en anden person. Biometriske eller adfærdsmæssige data refererer til målinger af unikke fysiske eller adfærdsmæssige egenskaber om en person.
Endelig refererer en ændring af kroppens funktion til en forstærkning eller modifikation af, hvordan brugerens krop præsterer, såsom en ændring i kognitiv forbedring og hukommelsesforbedring leveret af en hjerne-computer-grænseflade, eller evnen til at optage det, brugeren ser gennem en intraokulær linse, med et kamera.

IoB-enheder kræver generelt, men ikke altid, en fysisk forbindelse til kroppen (f.eks. bæres de, indtages, implanteres eller på anden måde fastgøres til eller indlejres i kroppen, midlertidigt eller permanent).
Mange IoB-enheder er medicinsk udstyr, der er reguleret af den amerikanske fødevare- og lægemiddelstyrelse (FDA).3 Figur 1 viser eksempler på teknologier i IoB-økosystemet, der enten allerede er tilgængelige på det amerikanske marked eller er under udvikling.

Enheder, der ikke er forbundet til internettet, såsom almindelige hjertemonitorer eller medicinske ID-armbånd, er ikke inkluderet i definitionen af IoB. Implanterede magneter (et nicheforbrugerprodukt, der bruges af dem i det såkaldte bodyhacker-miljø) er heller ikke. beskrevet i næste afsnit), som ikke er forbundet til smartphone-applikationer (apps), fordi selvom de ændrer kroppens funktionalitet ved at give brugeren mulighed for at registrere elektromagnetiske vibrationer, indeholder enhederne ikke software. Tendenser inden for IoB-teknologier og yderligere eksempler diskuteres yderligere i næste afsnit.

Nogle IoB-enheder kan falde ind og ud af vores definition på forskellige tidspunkter. For eksempel ville en Wi-Fi-forbundet smartphone i sig selv ikke være en del af IoB; men når en sundhedsapp er installeret, der kræver forbindelse til kroppen for at spore brugeroplysninger, såsom puls eller antal skridt, vil telefonen blive betragtet som IoB.

Vores definition har til formål at omfatte hurtigt udviklende teknologier, der har potentiale til at medføre de forskellige risici og fordele, der diskuteres i denne rapport. Vi fokuserede på at analysere eksisterende og nye IoB-teknologier, der synes at have potentiale til at forbedre sundheds- og medicinske resultater, effektivitet og menneskelig funktion eller ydeevne, men som også kan bringe brugernes juridiske, etiske og privatlivsmæssige rettigheder i fare eller udgøre personlige eller nationale sikkerhedsrisici.

I forbindelse med denne forskning har vi udført en omfattende litteraturgennemgang og interviewet sikkerhedseksperter, teknologiudviklere og IoB-fortalere for at forstå de forventede risici og fordele. Vi havde værdifulde diskussioner med eksperter på BDYHAX 2019, en årlig konference for bodyhackere, i februar 2019, og DEFCON 27, en af verdens største hackerkonferencer, i august 2019.
I denne rapport diskuterer vi tendenser i teknologilandskabet og skitserer fordele og risici for brugeren og andre interessenter. Vi præsenterer den nuværende status for styring, der gælder for IoB-enheder og de data, de indsamler, og konkluderer ved at tilbyde anbefalinger til forbedret regulering for bedst at afbalancere disse risici og fordele.

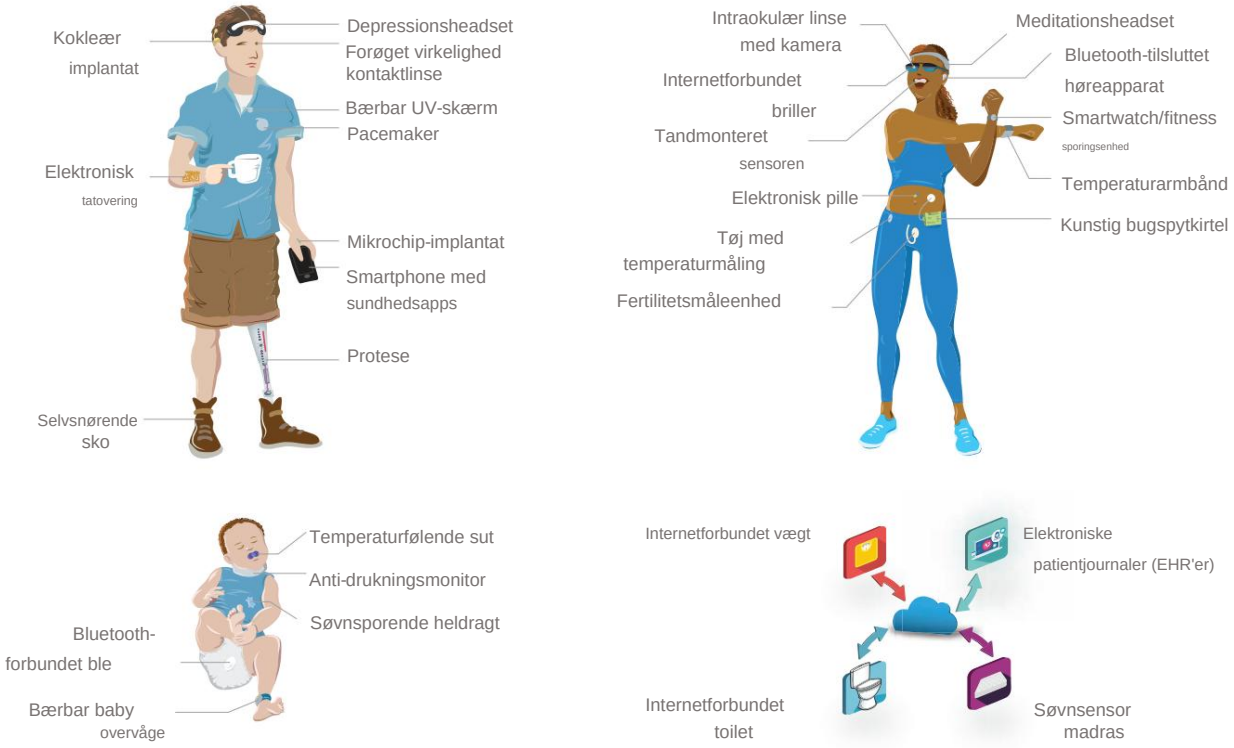
Et fremvoksende landskab af enheder og ideer

Tingenes Internet

IoB er tæt forbundet med IoT,4 som heller ikke har nogen universel definition; IoT-enheder har dog

Machine Translated by Google

FIGUR 1
Eksempler på IoB



flere bredt anerkendte karakteristika. For det første er IoT-enheder forbundet til internettet enten direkte eller via et lokalt netværk. For det andet har de mindst én af følgende funktioner: evnen til at forårsage eller registrere en fysisk ændring, til direkte at hente information fra eller give information til mennesker eller til at hente eller gemme data. Endelig skal IoT-enheder interagere for at give brugeren en fordel. For eksempel kan en pære programmeres til at tænde ved skumringstid uden at være forbundet til et netværk. Den bliver kun en del af IoT, når den er forbundet til en anden IoT-enhed, f.eks. en smartphone, som derefter giver en bruger mulighed for at tænde lyset uden at være hjemme. Baseret på vores definitioner er enhver IoT-enhed en IoT-enhed.

Vores definition af IoB omfatter teknologier fra det, der ofte kaldes sundhedsvæsenets Internet of Things (Healey, Pollard og Woods, 2015), selvom ikke alle IoT-enheder til sundhedsvæsenet vil blive betragtet som en IoB-enhed. Elektroniske patientjournaler, robotkirurgiske systemer og enheder, der bruges til medicinsk behandling, såsom smarte ventilatorer, er alle en del af IoB-økosystemet, fordi De indsamler brugeroplysninger eller ændrer kroppens funktion. Et hospitals "smarte" køleskab, der bruges til opbevaring af vacciner, og som kan være forbundet til et netværk og advare personalet, hvis lageret er lavt, er dog ikke en IoB-enhed, fordi den ikke opfylder vores definition.

Transhumanisme, bodyhacking, biohacking og mere

IoB er relateret til adskillige bevægelser uden for formel sundhedspleje med fokus på at integrere menneskekroppen med teknologi. Dernæst opsummerer vi nogle af disse koncepter,5 selvom der er megen overlapning og gensidig udskiftelighed mellem dem.

Transhumanisme er en verdensanskuende og politisk bevægelse, der går ind for menneskehedens transcendens ud over nuværende menneskelige evner. Transhumanister ønsker at bruge teknologi, såsom kunstige organer og andre teknikker, til at stoppe aldring og opnå "radikal livsforlængelse" (Vita-Moore, 2018). Transhumanister kan også søge at modstå sygdom, forbedre deres intelligens eller modvirke træthed gennem

Machine Translated by Google

kost, motion, kosttilskud, afslapningsteknikker eller nootropika (stoffer, der kan forbedre kognitiv funktion).

Bodyhackere, biohackere og cyborgs, der nyder at eksperimentere med kropsforbedring, omtaler ofte sig selv som grindere. De kan identificere sig som transhumanister eller ej. Disse udtryk bliver ofte brugt i almindelig brug, men nogle skelner mellem dem (Trammell, 2015). Bodyhacking

refererer generelt til at modificere kroppen for at forbedre ens fysiske eller kognitive evner. Nogle former for bodyhacking er rent æstetisk. Hackere har implanteret horn i deres hoveder og LED-lys under deres hud. Andre hacks, såsom at implantere RFID-mikrochips i ens hånd, har til formål at forbedre funktionen, så brugerne kan låse døre op, tage offentlig transport, gemme nødkontaktoplysninger eller foretage køb med et enkelt armbevægelse (Baenen, 2017; Savage, 2018). En bodyhacker fjernede RFID-mikrochippen fra sin bils nøglebrik og fik den implanteret i sin arm (Linder, 2019). Et par bodyhackere har implanteret en enhed, der er en kombineret trådløs router og harddisk, der kan bruges som en node i et trådløst mesh-netværk (Oberhaus, 2019). Nogle former for bodyhacking er af medicinsk karakter, herunder 3D-printede proteser og gør-det-selv kunstige bugspytkirtler.

Andre igen bruger udtrykket om enhver metode til at forbedre helbredet, herunder bodybuilding, kost eller motion.

Biohacking betegner generelt teknikker, der modificerer de biologiske systemer hos mennesker eller andre levende organismer. Dette spænder fra bodybuilding og nootropika til udvikling af kure mod sygdomme via selveksperimentering til genetisk manipulation af mennesker gennem CRISPR-Cas9-teknikker (Samuel, 2019; Griffin, 2018).

Cyborgs, eller kybernetiske organismer, er mennesker, der har brugt maskiner til at forbedre intelligensen eller sanserne. Neil Harbisson, en farveblind mand, der kan "høre" farver gennem en antenne implanteret i hans hoved, der spiller en melodi for forskellige farver eller bølgelængder af lys, er anerkendt som den første person, der er blevet juridisk anerkendt af en regering som cyborg, ved at få lov til at have sit pasbillede inkluderet i sit implantat (Donahue, 2017).

Fordi IoB er et vidtrækkende felt, der krydser hinanden med gør-det-selv kropsmodifikation, forbrugerprodukter og medicinsk behandling, er det afgørende at forstå fordele og risici.

IoB-teknologier

IoB-teknologi har udviklet sig hurtigt på tværs af en række medicinske og forbrugermæssige applikationer, hvor etablerede medicinalvirksomheder og store teknologifirmaer i stigende grad er blevet tilsluttet af nyere IoB-startups. I dette afsnit præsenterer vi eksempler på IoB-enheder for at demonstrere udvalget af teknologier, der er tilgængelige eller under udvikling.

Medicinske anvendelser af IoB

I løbet af det seneste årti har fremskridt inden for medicinsk teknologi og datalogi ført til en betydelig vækst i internetbaserede medicinske apparater, der lover bedre og mere præcise data til at understøtte patientpleje og forbedret sundhedseffektivitet. Disse apparater bruges til en række forskellige sygdomme og tilstande, herunder diabetes, anfald og Parkinsons sygdom.

Tabel 1 viser eksempler på internetaktiveret medicinsk udstyr, der kan implanteres, og tabel 2 viser nogle, der er bærbare eller fritstående;6 alle disse IoB-enheder er allerede i brug.

Forbrugerapplikationer af IoB

Forbrugermarkedet for IoB er vokset hurtigt med en række nye enheder tilgængelige eller under udvikling, der har til formål at forbedre hverdagens sundhed og komfort og tilbyde andre bekvemmeligheder.

Tabel 3 viser nogle eksempler.

Fremtidige tendenser: Mere forbindelse, Flere teknologier

Fremskridt inden for internetteknologi og -forbindelse vil gøre det muligt for mange flere IoB- og IoT-enheder at oprette forbindelse til hinanden og med langt højere hastigheder. Femte generations mobile telekommunikationsnetværk, 5G, kan understøtte omkring 1 million enheder pr. kvadratfod sammenlignet med det tidligere 4G-netværk, som kan understøtte omkring 4.000 enheder i samme område (Zaino, 2019). Wi-Fi 6, den næste generation af Wi-Fi

Machine Translated by Google

TABEL 1
Eksempler på implanterbare medicinske IoB-teknologier

Type af IoB	Beskrivelse
Kunstig bugspytkirtel	Systemet med kunstig bugspytkirtel integrerer kontinuerlig glukosemonitor (CGM) og insulinpumpeteknologi med AI-algoritmer, der automatiserer insulindosering baseret på input fra CGM'en (Boughton og Hovorka, 2019). Nogle diabetikere har opsøgt forældede insulinpumper for at hacke en sikkerhedsfejl, der gør det muligt at forbinde pumpen med en CGM til en gør-det-selv kunstig bugspytkirtel (Zhang, 2019).
Hjerne-computer-grænseflader (BCI'er)	BCI'er bruger elektroder, der forbinder signaler fra hjernen til en computer. De kan enten være implanteret i hjernen eller ikke-invasive (bærbare eller fastgjort til kraniet). BCI'er under udvikling sigter mod at læse og skrive hele ord direkte fra hjernen eller styre proteser fra sindet ("Imagining a New Interface", 2019; Etherington, 2019).
Hjernens elektriske signaler for Parkinsons sygdom	Dyb hjernestimulation – en kirurgisk procedure, hvor elektroder implanteres i en del af hjernen og forbindes til en lille elektrisk enhed implanteret i brystet – blev først godkendt til brug hos Parkinsons-patienter i USA i 2002 (LeMoyne et al., 2019). I de senere år har nye fremskridt som trådløs styring via en smartphone gjort teknologien mere præcis og personlig. Retningsbestemte ledninger gør det muligt for hver patients læge at målrette behandlingen mod specifikke områder af hjernen (Okun, 2019). En smartphone-app giver patienten mulighed for at justere indstillinger for at optimere daglige aktiviteter.
Cochlear-apparater	Et cochlear-implantat er en elektronisk enhed, der delvist genopretter hørelsen gennem en lydprocessor, der placeres bag øret for at opfange lydsignaler. Processoren sender disse signaler til en modtager, der er implanteret under huden, og som derefter stimulerer hørenerven (Slager et al., 2019). I juni 2017 blev det første implantat med trådløs forbindelse til smartphones godkendt af FDA. Denne enhed gør det muligt for patienter at overvåge hørelsen, justere indstillinger, se personlig høreinformation og finde manglende lydprocessorer fra deres smartphones.
Implanterbar hjertepacing	Nyere pacemakere, implanterbare defibrillatorer og ventrikulære hjælpeenheder kan give information i realtid og kontinuerligt om en patients hjertesvingninger og muliggøre fjernstyring af apparater for at automatisere tekniske kontroller, såsom batteristatus, ledningsimpedans og registrerings- eller pacingtærskler (Stachel et al., 2013).
Implanterbar glukose skærme	CGM'er måler blodsukker via en sensor placeret under huden, og sensoren sender aflæsninger via Bluetooth til håndholdte modtagere eller en smartphone-app. Når glukoseniveauet er for højt eller for lavt, modtager patienterne notifikationer, så de kan justere deres insulin eller øge deres blodsukkerniveau (FDA, 2018b).
Implanterbare smarte stents	Stents bruges traditionelt til at genåbne tilstoppede blodkar. Smarte stents muliggør kontinuerlig overvågning af blodgennemstrømningen på tværs af stenten for at advare sundhedspersonale om muligheden for nye tilstopninger (Chen et al., 2018).
Spiselige digitale piller	I 2017 godkendte FDA den første digitale pille: aripiprazoltabletter med en indtagelig sensor indlejret i pillen, der registrerer, at medicinen blev taget. Systemet fungerer ved at sende en besked fra pillens sensor til et bærbart plaster, der sender informationen til en mobilapp, så patienter kan spore indtagelsen af medicinen på deres smartphones. Patienter kan også give deres omsorgspersoner og læge adgang til informationen via en webbaseret portal (Trauth og Browning, 2018). Andre indtagelige digitale piller er nu tilgængelige, herunder orale onkologiske lægemidler med en digital sensor til at spore adhærens, dosering og patientaktivitetsniveauer for at udvikle bedre doseringsregimer til kemoterapier.

teknologi forventes også at forbedre forbindelsen ved at give flere enheder mulighed for at overføre data og kommunikere med routere samtidigt (Kastrenakes, 2019). Satellitinternet udvikles for at forbedre internettilgængeligheden, herunder i fjerntliggende områder, ved at placere tusindvis af satellitter i lavt kredsløb om Jorden (Grush, 2019; Staedter, 2019). Disse fremskridt vil gøre det muligt for forbrugernes IoT-teknologier, såsom smart home-systemer, at oprette forbindelse til IoB-enheder, så for eksempel ens smarte termostat vil vide, hvornår du er hjemme, smart tøj og kan automatisk regulere temperaturen i hendes hjem. Bedre tilslutningsmuligheder og den udbredte indpakning af IoB i smartphones og apparater – hvoraf nogle kan indsamle data uden brugerens viden – vil øge digital sporing af brugere på tværs af en række adfærdsmønstre.

Nogle enheder under udvikling – såsom augmented reality-kontaktlinser eller direkte hjerneskrivning – har potentiale til at ændre det sociale betydeligt ved at muliggøre optagelse og

Machine Translated by Google

TABEL 2

Eksempler på bærbare og fritstående medicinske IoB-teknologier

Type af IoB	Beskrivelse
EHR'er	Digitale lagre af en patients medicinske historie (herunder behandlingshistorik, genetiske data, data fra bærbare enheder og andre biometriske oplysninger), der tilbyder patientcentreret information i realtid med det samme til autoriserede brugere (Dinh-Le et al., 2019; Office of the National Coordinator for Health Information Technology, 2019).
Fritstående infusionspumper	Programmerbare infusionspumper og systemer til reduktion af dosisfejl anvendes nu almindeligvis på hospitaler til intravenøs medicinafgivelse. Disse systemer integrerer medicindatabaser med infusionspumper og muliggør automatisering af alarmsystemer, der advarer sundhedspersonale, når der er opstået programmeringsfejl (Giuliano et al., 2018). Andre systemer forbinder infusionspumpen til patientens elektroniske patientjournal, hvilket fjerner behovet for at programmere pumpen.
Sensorudstyrede hospitalssenge	Senge, der indeholder sensorer til kropstemperatur, hjerterytme, blod, ilt, tryk eller andre data, der sendes til hospitalets centrale system og gør det muligt for sundhedspersonale øjeblikkeligt at overvåge patienters vitale data (Bentley, 2018).
Bærbare insulinpumper	Computerbaserede enheder, der leverer insulin kontinuerligt i et forsøg på at efterligne normal insulinfrigivelse fra bugspytkirtlen. Programmerbar insulinadministration kan integreres og suppleres med CGM-biosensorer for at give glykæmisk kontrol i realtid ("How Insulin Pumps Work", 2019).
Bærbare proteser	Proteser med elektroniske sensorer til at registrere små muskelbevægelser for at betjene proteser (Zlotolow og Kozin, 2012). Nogle er internetbaserede og sender feedback til producenter for at forbedre teknologierne; nogle kan spore vitale tegn (Yang et al., 2017).
Bærbare anfaldsmonitorer	Ure og andre bærbare enheder, der kontinuerligt overvåger brugeren og advarer familiemedlemmer og omsorgspersoner ved opståen af unormale bevægelsesmønstre, der ligner dem, der er forårsaget af anfald, såsom dem, der er forårsaget af epilepsi (Wicklund, 2018).

genafspilning af alle en persons interaktioner. Neuroenheder til hjernelæsning og signalering findes allerede på markedet, men forbedrede hjerneteknologiske grænseflader kan med succes forbedre kognition, hukommelse og kontrol. Hjernelæsning og -skrivning kan i sidste ende bruges til at påvirke folks tanker i velgørende eller ondsindede hensigter (CPDP Conferences, 2018).

Militært personale har vist interesse for IoB-teknologier til at spore soldaters helbred og velbefindende, forbedre deres kognitive og fysiske evner, forbedre træning og muliggøre forbedrede krigsføringsevner – for eksempel med augmented reality-headset eller teknologibaserede exoskeletter, der sporer krigsfolks fysiske egenskaber og muligvis også deres sindstilstand.

Militært har søgt at udvikle neuro-enheder, der muliggør kontrol over fysiske systemer – for eksempel afkodning af motoriske kontrolsignaler fra hjernen, så en pilot kan flyve et fly ved hjælp af sine tanker (Emondi, udateret). Sådanne muligheder ville muliggøre hurtigere beslutninger på slagmarken, men kan også introducere nye risici for krigsførelse, såsom cyberangreb, der direkte påvirker en soldats hjerne (Binnendijk, Marler og Bartels, kommende).

Data fra IoB kan også anspore medicinske, militære eller andre fremskridt på uventede måder. For eksempel blev det i juni 2019 rapporteret, at det amerikanske forsvarsministerium har en infrarød laser, der kan registrere en persons unikke hjertesignatur (måling af hjertets elektriske rytmer) med over 95 procents nøjagtighed fra en afstand på 200 meter, selv gennem bestemt tøj (Doffman, 2019). Hvis en database med elektroniske patientjournaler med hjertesignaturer var tilgængelig, kunne denne laser bruges til at overvåge patienters hjertehændelser på et hospital eller til at identificere individuelle kombattanter i en krigszone på afstand med stor nøjagtighed (Hambling, 2019).

Evaluering af sundhedsfordelene ved Internet of Bodies

I 2025 vil der være mere end 41 milliarder aktive IoT-enheder (International Data Corporation, 2019), der genererer 2,5 quintillion bytes data dagligt (Marr 2018) om miljø, transport, geolokation, kost, motion, biometri, sociale interaktioner og hverdagslivet (Faiola og Holden, 2017; Piwek et al., 2016). Denne eksplosion i IoT-enheder vil

Machine Translated by Google

TABEL 3
Eksempler på forbruger-IoB-teknologier

Type af IoB	Beskrivelse
Opmærksomhedsmonitorer	Briller, der bruger hjerneaktivitet og øjenbevægelser til at spore opmærksomhed. De er designet til brug i skoler eller under kørsel og giver lyd- eller haptisk feedback, når de fornemmer, at brugeren er uopmærksom (Massachusetts Institute of Technology Media Lab, 2019).
Kropsimplanteret sensorer	Vævsintegrerede biosensorer under udvikling kan muligvis give mere præcis og omfattende biotracking end traditionelle wearables. Disse implanterede sensorer kan også have yderligere funktionalitet, såsom en hudtransplanteret grænseflade, der gør det muligt for brugeren at fjernstyre andre enheder (Khan, 2019). Tandmonterede RFID-sensorer under udvikling vil spore information om glukose, salt og alkohol, som brugeren indtager (Silver, 2018).
Tøj med sensorer	Tøj, der indeholder sensorer, der registrerer kropstemperaturen og tilpasser sig for at holde bæreren komfortabel. Der findes også produkter til spædbørn, såsom bleer, der bruger en Bluetooth-forbundet app til at registrere og rapportere afføring (Waters, 2019).
Kvindelige teknologiprodukter	"FemTech"-produkter er teknologier, der har til formål at forbedre kvinders sundhed. De omfatter app-forbundne bærbare enheder, der måler livmoderhalsslim for at spore fertiliteten, enheder, der hjælper kvinder med at styrke deres bækkenbund ved at opmuntre til og spore kegeløvelser, og sensorer, der måler veer under fødslen (Jaramillo, 2019).
Fritstående internetforbundne møbler og apparater	Fritstående internetforbundne møbler og apparater til forbrugere, der sporer og giver feedback om brugerens velbefindende (IoB) derhjemme. Disse omfatter toiletter, der overvåger urinflow og sukkerniveauer og rapporterer resultater via en app (Marr, 2019a); vægte, der er integreret med sundhedsapps for at spore og analysere udsving i kropsvægt, kropsmasseindeks og vandvægt (Ross, 2019); og senge udstyret med sensorer, der opretter forbindelse til søvnsporingsapps for at indsamle og registrere data om søvnmønstre (Appleby, 2019).
Implanterbare mikrochips	RFID- og nærfeltskommunikationsmikrochips (NFC) implanteret i menneskekroppen for at lagre information, såsom navn og adresse (svarende til de chips, som mange kæledyrsejere sætter i deres hunde). Nogle kan programmeres til at låse døre op eller betale for varer, svarende til smartphone-betalingssystemer (Gillan, 2019).
Mental og følelsesmæssig sensorer	Fritstående og bærbare sensorer kan vurdere en brugers mentale og følelsesmæssige tilstande ved at analysere ansigtsudtryk, stemmeintonationer og andre lyd- og visuelle signaler (Day, 2019; Clymo, 2018).
Syns- og høreapparater	Syns- og høreapparater til at genoprette eller forstærke opfattelsen og give mulighed for at optage video og lyd. I 2017 blev det første amerikanske patent på en implanterbar intraokulær linse med videokamera og trådløse funktioner udstedt (Strathspey Crown, 2017). "Hearables" er ikke kun beregnet til at hjælpe med høretab, men også til at oprette forbindelse til virtuelle smartphone-assistenter for at registrere, om brugeren er faldet, og andre adfærdsindikatorer (Tibken og Cheng, 2018).
Bærbare sundhedssporere	Armbånd, ure, ringe og smartphone-apps, der sporer skridt, puls, søvnmønstre og andre fysiske data, såsom hvor meget alkohol bæreren har indtaget (Turk, 2019). Disse enheder fungerer ved hjælp af avancerede accelerometre og andre sensorer, der kan oversætte bevægelse til digitale målinger. Mange enheder tilbyder også dataanalyse og displays, der giver detaljerede oplysninger i tilgængelige former.
Bærbare neuro-enheder	Neuroenheder, der kan bæres på hovedet, registrerer og overvåger hjerneaktivitet og stimulerer hjernen gennem elektriske signaler. Nogle bruges til at opfordre brugeren til at udføre hjerneøvelser. Andre kan sende elektriske signaler til hjernen for at behandle tilstande som kroniske smerter, depression, ADHD og posttraumatisk stresslidelse (Coates McCall et al., 2019).

resultere i yderligere popularitet af IoB-enheder. IoB kan tilbyde subjektive fordele, såsom glæde og bekvemmelighed, men her fokuserer vi på at evaluere, om sundhedspersonale med øget forståelse af patienters IoB-information kan forbedre forebyggende sundhedsbehandling, opdage sygdom tidligere, forbedre nøjagtigheden af diagnoser og behandle sygdomme mere effektivt i det formelle sundhedssystem.

I de følgende afsnit illustrerer vi eksempler af medicinsk og sundhedsmæssig IoB og evidensen vedrørende deres fordele. IoB kan muliggøre bredere adgang til sundhedspleje ved at muliggøre billig "distribueret" eller "demokratiseret" sundhedspleje eller ved at mindske behovet for risikabel eller dyr medicinsk intervention. Gennem større sundhedsbevidsthed, forbedret forebyggelse og mere effektiv intervention har IoB endda potentiale til at reducere sundhedsomkostningerne. Men det er

Machine Translated by Google

Det er vigtigt at bemærke, at mange IoB-teknologier er for nye til at have udviklet et klinisk evidensgrundlag for langsigtede resultater. I stedet rapporteres fordelene hidtil i vid udstrækning som forbedring af den daglige effektivitet for udbydere. Det vil være nødvendigt at spore evidensgrundlaget, efterhånden som IoB bliver mere mainstream, for at forstå de sande effekter af disse enheder på kliniske resultater.

Effekter på præcisionsmedicin og Præcisions folkesundhed

Præcisionsmedicin og præcisionsfolkesundhed (Dolley, 2018) opstod for at udvikle målrettede sundhedsinterventioner for at imødekomme unikke behov hos specifikke befolkningsgrupper. Præcisionsmedicin muliggøres af (1) en stor mængde undergruppespecifik forskning, der tyder på, at forskellige sundhedsinterventioner ikke er bredt effektive, og at stratificerede strategier kan være nødvendige for at forbedre lighed; (2) stigningen i omfangrige, præcise, kontinuerlige og longitudinelle data genereret af IoB, der giver hidtil uset indsigt i individers oplevelser; og (3) samtidig modning af datavidenskab, som bevæger sig ud over grove tidsskalaer og enkeltniveau-effekter til raffinerede, multitidsskala-, multiniveau- og intersektionelle analyser, der bedre tager højde for komplekse interaktioner mellem sociale determinanter, adfærd og sundhed. Disse faktorer tyder på, at i det omfang IoB-enheder muliggør præcisionsmedicin, kan de forbedre sundhedsresultaterne for sårbare eller understuderede befolkningsgrupper.

IoB-enheder indsamler PGHD på stort set alle aspekter af livsstil og adfærd, hvilket skaber en skattekiste af information, der potentielt kan fremme forståelsen af langsigtet befolkningssundhed og præcise folkesundhedsinterventioner. PGHD indsamlet af IoB-enheder muliggør kontinuerlig overvågning af sundhedsstatus i realtid, samt indsamling af longitudinelle data uden for - eller i tillæg til - den intermitterende overvågning, der finder sted i kliniske miljøer (Lai et al., 2017). PGHD kan informere korrelationer mellem individuel adfærd, sociodemografi og faktorer på befolkningsniveau og afdække de komplekse forhold mellem akutte og kroniske stressfaktorer, kost, livsstil og generel sundhed.

Imidlertid er PGHD kun så effektive som de analyser, der er udviklet til at omsætte enorme mængder ustruktureret, forskelligartet data til meningsfuld sundhedsindsigt og interventioner. Maskinlæring, AI og andre datavidenskabelige teknikker bruges ud over traditionel statistik til at genkende mønstre i – og lave forudsigelser baseret på – store, empiriske datasæt (Lupton, 2013; Lupton, 2014). AI er med succes blevet indarbejdet i beslutningsstøtte inden for dataintensive specialer såsom radiologi, patologi og oftalmologi (Yu og Kohane, 2019). I modsætning til hypotesedrevne designs muliggør datavidenskab netværksbaserede, flerniveau-korrelationer af flere variabler på sundhedsresultater for at udvikle komplekse risikoforudsigelser, der kan hjælpe med beslutningstagning. Det muliggør identifikation af digitale sundhedsindikatorer, der kan bruges til at overvåge, påvirke og opretholde sunde vaner i realtid. For eksempel viser nyere undersøgelser, at individuelle ændringer i hyppighed og intensitet af fysisk aktivitet kan forudsige depression (Kumar et al., 2018), og at lyddata indsamlet fra folks mobiltelefonsamtaler kan forudsige kognitiv svækkelse (Stück et al., 2018).

Sådanne studier fremhæver en stor mulighed for at bruge IoB til at skabe en synergistisk feedback-loop mellem forskere, sundhedspersonale og forbrugere.

Racemæssige og etniske minoriteter, socioøkonomiske I dag oplever befolkningsgrupper, der er blevet udsat for dårligt stillede og diskriminerede befolkningsgrupper, fortsat uforholdsmæssigt negative sundhedsresultater (National Center for Health Statistics, 2016), på trods af årtiers forskning, der korrelerer individuelle sociale sundhedsdeterminanter, såsom demografi (f.eks. alder, køn, race), sociale eller befolkningsmæssige karakteristika (f.eks. beskæftigelse, nabolag, bolig) og tilhørende adfærd (f.eks. kost, motion, stoffer, alkohol) med variationer i sundhedsresultater (Marmot, 2005). Mange folkesundhedstilgange bruger stadig befolkningsgennemsnit til at skabe "one-size-fits-all"-interventioner for at øge sandsynligheden for at opnå de bedste resultater for de fleste mennesker (Glasgow, Kwan og Matlock, 2018; Braveman et al., 2005), hvilket kan bidrage til uforholdsmæssigt negative resultater. IoB kan bidrage til at bekæmpe dette ved yderligere at muliggøre præcisionsmedicin og præcisionsfolkesundhed.

Machine Translated by Google

Elektroniske sundhedsjournaler

EHR'er promoveres af Office of the National Coordinator for Health Information Technology, en del af det amerikanske sundhedsministerium, for at forbedre interoperabiliteten af sundhedsdata.
EHR'er er digitale lagre af en patients medicinske historie, der tilbyder patientcentreret information i realtid til autoriserede brugere. Selvom EHR'er indeholder patienters medicinske og behandlingsmæssige historier, er de designet til at gå ud over standard kliniske data indsamlet på en læges kontor og kan omfatte adfærd, levevilkår og familiehistorie.

Avancerede elektroniske patientjournaler kan også indeholde genetiske data og data fra bærbare enheder og en række andre kilder.

EHR'er fremmer evidensbaseret praksis ved at integrere kliniske retningslinjer og automatiseringsværktøjer, der forsyner udbydere med opdaterede anbefalinger til patientpleje (Allen-Graham et al., 2018). De har vist forbedret produktivitet og ressourcestyring for hospitaler og forbedret kvalitet af plejen for patienter (Entzeridou, Markopoulou og Mollaki, 2018). For eksempel rapporterede 88 procent af praksisserne i en nylig national undersøgelse, at deres EHR giver kliniske fordele for patienterne, og 75 procent rapporterede, at EHR'er muliggør bedre plejelevering. Årsager til kliniske fordele omfattede reduktion af medicineringsfejl, forbedret patientsikkerhed og forbedret personlig håndtering af pleje (Jamoon et al., 2012).

Efterhånden som IoB leverer rigere og mere forskelligartede data til Med EHR'er er der grund til at forvente, at de vil hjælpe forskere og klinikere med at forstå sammenhængene mellem miljø, adfærd, sundhed og sygdom.

Indlæggelsesansøgninger

IoB kan muliggøre bedre styring af pleje og medicinlevering på hospitaler. Sammenkoblede maskiner, der deler data (f.eks. elektroniske patientjournaler, klinisk beslutningsstøtte, medicindispensering, ventilatorer, infusionspumper, hospitalssenge), kan reducere fejl og give hospitalspersonalet mulighed for at bruge mindre tid på at søge efter patientjournaler eller medicinoplysninger, spore regler og opgøre forsyninger.

IoB kan muliggøre bedre styring af pleje og medicinlevering på hospitaler.

For eksempel bruges programmerbare infusionspumper og systemer til reduktion af dosisfejl nu almindeligt på hospitaler til at levere intravenøs medicin på en præcis og kontrolleret måde. Medicineringsfejl kan dog opstå som følge af brugerfejl i programmeringen af pumpen. Nyere infusionspumper muliggør algoritmisk automatisering af alarmsystemer, der advarer sundhedspersonale, når der er opstået programmeringsfejl, ved at matche medicin med doseringsretningslinjer (Giuliano et al., 2018). Intravenøs klinisk integration (Downey et al., 2018) tager dette et skridt videre – en læge indtaster en medicinordre i det elektroniske patientjournalsystem, og denne ordre transmitteres direkte til infusionspumpen med de korrekte flowhastigheder og doseringer.

Sensorudstyrede hospitalssenge udnytter den store mængde tid, patienter tilbringer i sengen, til at spore deres vitale tegn og uploade data til deres elektroniske patientjournal. Sensorer kan måle kropstemperatur, puls, blod, ilt, tryk, væskeindtag og -output og andre indikatorer. Behandlere kan eksternt evaluere og overvåge deres patienter og modtage advarselsmeddelelser i tilfælde af pludselig ændring i patientens status (Downey et al., 2018). En systematisk gennemgang viste, at kontinuerlig telemetriovervågning på hospitaler via sensorudstyrede senge og andre systemer forbedrede patientresultaterne og reducerede tiden brugt på intensiv pleje for patienter i modsætning til intermitterende overvågning (Downey et al., 2018), hvilket tyder på, at bred implementering af ikke-invasiv overvågning kan forbedre patientplejen.

Ambulant behandling og overholdelse Ledelse

Det er påvist, at IoB-behandlingsmonitorering hjælper patienter med at overholde deres behandlingsplaner.

Machine Translated by Google

samtidig med at lægerne kunne spore overholdelse af recepter. I 2017 godkendte FDA den første digitale pille: en aripiprazoltablet med en indtagelig sensor indlejret i pillen, der registrerer, at medicinen blev taget. Produktet er godkendt til behandling af skizofreni, akut behandling af maniske og blandede episoder forbundet med bipolar I-lidelse og til brug som tillægsbehandling af depression hos voksne. Behandlingsadhærens er afgørende for sådanne lidelser og betragtes som den største enkeltstående faktor, der forudsiger tilbagefald hos patienter (Papola, Gastaldon og Ostuzzi, 2018). Systemet fungerer ved at sende en besked fra pillens sensor til et bærbart plaster.

Plasteret sender informationen til en mobilapplikation, så patienterne kan spore indtagelsen af medicinen på deres smartphone. Patienterne kan også give deres omsorgspersoner og læge adgang til informationen via en webbaseret portal (Trauth og Browning, 2018).

Med udgangspunkt i succesen med den digitale pille er der også blevet udviklet et oralt onkologisk lægemiddel med en digital sensor til at spore overholdelse, dosering og patientaktivitetsniveauer for at forbedre doseringsregimer for kemoterapier. Til sidst kan andre sådanne IoB-aktiverede behandlinger give sundhedspersonale og omsorgspersoner ny indsigt, muliggøre fjernbehandling af patienter, undgå hospitalsindlæggelser og forbedre responsen på behandling (Plowman, Peters-Strickland og Savage, 2018).

Fjernovervågning af kroniske lidelser

Det globale fænomen med en aldrende befolkning (FN, 2015; Harper, 2006) har ført til en betydelig stigning i forekomsten og prævalensen af kroniske, ikke-smitsomme sygdomme (NCD'er). Hvert år dør næsten 41 millioner mennesker af NCD'er, hvilket repræsenterer 71 procent af alle globale dødsfald. NCD'er tegner sig for en uforholdsmæssig stor del af sundhedsudgifterne, da omtrent de dyreste 5 procent af patienterne tegner sig for omkring 50 procent af sundhedsomkostningerne (Verdenssundhedsorganisationen, 2018).

IoB er en lovende tilgang til udvikling af fjernovervågningssystemer til sundhed i realtid for ikke-smittsomme sygdomme (NCD)-patienter, primært diabetikere og hjertepatienter. Diabetes er endemisk i de fleste regioner i verden. Nylige udviklinger inden for kunstig bugspytkirtelteknologi, muliggjort af en række IoB-enheder, lover bedre glykæmisk kontrol og fjernovervågning af patienter (Garg et al., 2017).

Forskning har vist, at overvågning af vitale tegn kan bidrage til at reducere antallet af genindlæggelser ved at opdage anomalier tidligt og muliggøre passende og rettidige interventioner (Fanucci et al., 2013). FDA har godkendt et armbåndsur, der sporer atrieflimren og advarer patienter om, at de muligvis har brug for at se en læge (Apple, 2018). Derudover viste en undersøgelse foretaget af Center of Connected Health Policy, at fjernovervågning af hjertesvigtpatienter ved hjælp af IoB-enheder førte til en 50 procents reduktion i antallet af genindlæggelser efter 30 dage (Agboola et al., 2015). Det blev antaget, at tidlig opdagelse og intervention gennem fjernovervågning var de primære drivkræfter for reduktionen.

Redder liv gennem alarmer

IoB-enheder kan indsamle vigtige data for at give medicinske advarsler til læger, patienter og plejepersonale. FDA har godkendt et armbåndsur til overvågning af anfald, der registrerer unormale bevægelsesmønstre. Når dette ur registrerer en gentagen rystende bevægelse, der er karakteristisk for visse anfald, sender det automatisk sms- og telefonopkaldsadvarsler til patientens udpegede modtagere af advarsler. Kliniske undersøgelser viste, at uret var i stand til korrekt at identificere anfald hos både voksne og pædiatriske patienter med en næsten nul falsk positiv rate (Gutierrez et al., 2018).

IoB-enheder kan også vise sig nyttige til at vejlede behandlingen af dem, der ikke kan tale eller formulere deres symptomer eller tanker, såsom spædbørn, slagtilfældeofre eller demenspatienter, ved for eksempel at advare omsorgspersoner om betydelige ændringer i vitale tegn. Ældre borgere kan også drage fordel af f.eks. sensorer, der kan registrere fald og tilkalde nødtjenester. Forskere, der bruger sådan sensorteknologi, fandt ud af, at det endda var muligt at forudsige forekomsten af et fald baseret på brugerens gangmønstre (Scott, 2018).

Sygdomsovervågning

Sygdomsovervågning afhænger af dataindsamling fra et stort antal individer og hospitaler over store geografiske afstande. IoB egner sig til

Machine Translated by Google

særligt godt til dette formål (Steele og Clarke, 2013), fordi sensorer indbygget i smartphones, bærbare enheder og offentlige faciliteter som toiletter eller dørhåndtag alle kan bruges til at detektere tilstedeværelsen af sygdomme og spore dens spredning i hele befolkningen. Dette kan muliggøre intervention i forbindelse med epidemier eller pandemier som mæslinger, ebola eller influenza.

Særligt bemærkelsesværdigt er IoB-enheders evne til at bestemme antallet af personer, der har været i kontakt med en sygdom, men ikke er symptomatiske, de såkaldte tavse bærere, som er afgørende for at forstå sygdomsforekomsten.

IoB kan være en effektiv løsning på denne kritiske nævnerudfordring (Purcell et al., 2016) ved at muliggøre sporing og analyse af tavse bæreradfærd.

Usikkerheder i IoB-fordele: Hvordan Løfter stables op

Selvom mange fordele ved IoB er blevet realiseret i den formelle medicinske sektor, er der fortsat usikkerheder.

Praktiske realiteter kan forhindre mange IoB-løfter i at blive opfyldt, i det mindste på kort sigt – for eksempel har funktionel interoperabilitet mellem elektroniske patientjournaler været en udfordring (Sullivan, 2018), og overgangen er fortsat et igangværende arbejde. Sundhedspersonale har haft en blandet reaktion på andre patienttilgange til selvhjælp, såsom informationssøgning via online sundhedsfællesskaber (Rupert et al., 2014). Som med andre gør-det-selv-fænomener (f.eks. skiftet til automatiske pengeautomater) kan der være langsigtede ændringer.

til økonomisk aktivitet (som ændringer i forbrugsmønstre muliggjort af improviseret forbrug). Disse ændringer er måske for tidlige at forstå nu, men bør overvåges af forskere i takt med at IoB og anden digitalisering udvikler sig.

Evaluering af risiciene ved Kroppernes internet

Computersoftware er i sagens natur sårbar over for utilsigtede fejl eller ondsindet misbrug. Svagheder i kode kan udnyttes til at stjæle eller manipulere information indsamlet af enheden, forstyrre dens funktion eller på anden måde få den til at opføre sig på uventede eller utilsigtede måder. IoB-teknologier lider af de samme angrebsvektorer som andre IoT- og computerenheder, men IoB-enheder har øgede risici som følge af sammenløbet af flere egenskaber, herunder forbindelse til kroppen, typen og omfanget af de indsamlede oplysninger, og hvordan oplysningerne kan bruges. Tabel 4 opsummerer IoB-risici som en funktion af dem, der kan opnå uautoriseret, ulovlig eller uventet adgang til dataene eller, gennem enheden, til kroppen; forventede sårbarheder; og potentielle konsekvenser. De IoB-enheder, der sandsynligvis vil udgøre de farligste konsekvenser (højre kolonne i tabel 4), er dem, der besidder et stort antal sårbarheder (midterste kolonne i tabel 4), som kan udnyttes af adskillige aktører (venstre kolonne i tabel 4).

TABEL 4

IoB-risici: Uventet adgang, sårbarheder og Konsekvenser

Hvem kan få adgang?	Hvad er potentielle sårbarheder?	Hvad er mulige konsekvenser?
• Kriminelle • Hackere (f.eks. sikkerhedsforskere, hobbyister, ondsindede angribere) • Datamæglere • Datafusionscentre • Arbejdsgivere • Skoler • Sundhedsudbydere • Forsikringsselskaber • Producenter • Strafferetssystem • Regeringer	• Kropslig afhængighed af apparater for helbreds- eller funktionsmæssige årsager formål • Indsamling af følsomme data, besiddelse eller formidling • Internetforbindelse • Reguleringshuller • Hardware • Software	• Død eller fysisk skade som følge af funktionsfejl eller hacking • Globale og nationale sikkerhedsudfordringer • Databrud • Passiv indsamling eller deling af data uden informeret samtykke • Misbrug eller uventet brug af data • Personlig identifikation • Øgede uligheder i sundhed • Tvang til at acceptere enheder • Krænkelse af kroppens autonomi

Machine Translated by Google

Global, national og personlig sikkerhed Risici

I 2018 udgav fitnessfirmaet Strava detaljerede geolokationsoplysninger om brugernes træningsruter. Forsvarsministeriet havde opfordret til brug af sundhedssporingsenheder i et forsøg på at bekæmpe fedmeepidemien og gennemførte et pilotprogram, der uddelte fitnesstrackere til mere end 2.000 soldater i 2013 (Bushatz, 2013) og 20.000 soldater i 2015 (Lilley, 2015). De kort, Strava udgav, var så detaljerede og omfattende, at de potentielt afslørede skjulte militærbaser og lejre for amerikansk militært og civilt personel samt livsmønstrene for soldater (Hern, 2018). Efter hændelsen ændrede militæret sin politik og tillader ikke længere udsendte soldater at bruge sådanne apps eller enheder (Copp, 2018).

Dette er blot ét eksempel på, hvordan eksplosionen af innovation og anvendelse af IoB-enheder kan udgøre globale og nationale sikkerhedsrisici. Nogle af disse risici kan forudses. For eksempel overvejede læger muligheden for, at vicepræsident Dick Cheneys pacemaker kunne bruges til at myrde ham.

Cheneys originale pacemaker var udstyret med en trådløs overvågningsfunktion, som potentielt kunne hackes. I 2007 blev Cheneys enhed erstattet med en uden trådløs funktion (Vaas, 2013).
Andre sådanne IoB-risici er muligvis ikke så lette at forudse eller håndtere.

Forbindelse af internetforbundne enheder er udvikler sig i art og kvalitet og vil blive yderligere muliggjort af kommunikationsteknologier, såsom 5G, næste generations Wi-Fi og satellitinternet. Men kommunikationssystemer vil sandsynligvis blive mål for fjendtlige nationer og kriminelle hackere. Nye Wi-Fi-protokoller har allerede vist sig at have sikkerhedsbrister (Goodin, 2019);7 der er opstået bekymringer om 5G (Ng, 2019), især i betragtning af kinesiske leverandørers dominans inden for levering af hardware og tjenester globalt (Bryan-Low et al., 2019); og voksende counterspace-programmer i Kina og Rusland kan true amerikanske satellitbaserede systemer (Defense Intelligence Agency, 2019). Den øgede konnektivitet i IoT- og IoB-enheder kan give en øget angrebsflade, der introducerer flere sårbarheder gennem disse netværk.8

Udenlandske investeringer i og opkøb af amerikanske virksomheder har længe været en bekymring på grund af nationale sikkerhedsrisici. Committee on Foreign Investment in the United States (CFIUS) blev oprettet i 1975 for at analysere transaktioner, der kan have konsekvenser for amerikanske nationale interesser (Jackson, 2019). CFIUS kan anbefale en suspension eller et forbud mod investeringer i en amerikansk virksomhed, hvis det ville give en udenlandsk enhed mulighed for at opbevare eller indsamle følsomme personoplysninger om amerikanske borgere. Derfor skal eksterne investeringer i IoB-virksomheder undersøges nøje. I 2016 overtog det kinesiske firma Kunlun kontrollen over Grindr, en populær datingapp for homoseksuelle, men indvilligede i at sælge den i maj 2019 efter en CFIUS-undersøgelse (Wang, 2019). Selvom CFIUS ikke har oplyst specifikke grunde til sin modstand mod kinesisk ejerskab af Grindr-databaser, giver oplysninger om brugernes placering, beskeder og HIV-status anledning til bekymring for afpresning af amerikanske embedsmænd eller offentlige entreprenører (Bauerle Danzman og Gertz, 2019).

Ligesom udenlandsk besiddelse af data om amerikanernes datingvaner eller HIV-status kan bruges til skumle formål, mens amerikanske forbrugeres biometriske og sundhedsmæssige data kan udnyttes af modstandere, der kan indsamle data fra adskillige kilder for at opbygge detaljerede profiler af deres amerikanske mål. I maj 2019 blev kinesiske aktører tiltalt for identitetstyveri, computerhacking og sammensværgelse om at begå bedrageri i forbindelse med hackingen af Anthem i 2015, et af de største sundhedsforsikringsselskaber i USA (Groll, 2019; Larson, 2019). Dette brud kompromitterede data, hvoraf nogle var følsomme medicinske data, fra 80 millioner mennesker (Whittaker, 2019), herunder anslået halvdelen af alle amerikanske føderale ansatte (ThreatConnect Research Team, 2015). Desuden har Kina ifølge en rapport fra 2019 (Gryphon Scientific and Rhodium Group, 2019), der er udarbejdet for den amerikanske-kinesiske økonomiske og sikkerhedsmæssige gennemgangskommission, allerede direkte adgang til store mængder kliniske og genetiske data om amerikanske indbyggere via investeringer og partnerskaber med amerikanske sundhedsvirksomheder. Kina forfølger også en langsigtet strategi om at blive en førende inden for bioteknologi og gør hurtige fremskridt på området gennem tovejsinvesteringer med amerikanske virksomheder, forskningspartnerskaber med amerikanske institutioner og rekruttering af udenlandsk og kinesiskfødte forskere, der er blevet uddannet i

Machine Translated by Google

USA (Gryphon Scientific og Rhodium Group, 2019). Denne strategi kan muligvis gøre det muligt for Kina at øge sit fodfæste i adgangen til amerikanernes biometriske data, både på enkeltpersoners og delpopulationers niveau, hvad enten det er gennem kommercielle midler eller spionage.

Øget implementering af IoB kan også øge de globale geopolitiske risici, fordi overvågningsstater kan bruge IoB-data til at håndhæve autoritære regimer.
For eksempel bruger Kina DNA-data i et forsøg på at overvåge uighurer (Wee, 2019). Det er også blevet rapporteret, at Kinas sociale kreditvurderingssystem bruger enorme mængder aggregerede data, herunder sundhedsjournaler, om enkeltpersoner til at bestemme deres troværdighed og til at fremme ønsket adfærd (Marr, 2019b). Udbredt brug af IoB kan øge risikoen for fysisk skade, spionage og udnyttelse af data af modstandere.

Cybersikkerhedsrisici

Cybersikkerhedsrisici grupperes ofte i tre kategorier, kendt som CIA-triaden, for fortrolighed, integritet og tilgængelighed (Center for Internet Security, udateret). Fortrolighed betyder, at data kun kan ses af autoriserede enheder; integritet betyder, at de indsamlede data ikke er blevet manipuleret med; og tilgængelighed sikrer, at dataene er tilgængelige, når og hvor de er nødvendige.

I starten af 2019 var FDA ikke bekendt med nogen skader eller dødsfald som følge af ondsindede angreb eller kompromittering af tilsluttet medicinsk udstyr (FDA, 2019a).9 Sårbarheder i disse enheder kan dog utilsigtet forårsage fysisk skade eller udnyttes ondsindet til at forårsage skade eller død.
For eksempel findes der to velkendte sårbarheder i forbindelse med medicinsk udstyr i implanterbare defibrillatorer og insulinpumper, forårsaget af dårligt implementerede kommunikationsprotokoller mellem enheden og fjernovervågningssystemerne. I det første tilfælde blev der fundet en sårbarhed i den trådløse kommunikationssoftware i en almindelig implanterbar cardioverter defibrillator (FDA, 2019b). Denne sårbarhed kan gøre det muligt for en angriber at opfange kommunikationen mellem den implanterede enhed og de kliniske programmeringsenheder eller hjemmeovervågningsmaskiner på en måde, der kan muliggøre manipulation af data eller indsættelse af falske (ondsindede) kommandoer til den implanterede enhed. Tilsvarende opdagede en sikkerhedsforsker i 2016 tre sårbarheder i computerkoden til en insulinpumpe, der kunne give en angriber mulighed for at injicere ondsindede kommandoer og forårsage alvorlig skade (Beardsley, 2016).

Derudover er der bekymringer vedrørende det bredere økosystem, hvor IoB-enheder anvendes (Das, Zeadally og Wazid, 2017). En fysisk enhed, der er implanteret eller fastgjort til kroppen, vil trådløst oprette forbindelse til en overvågningsenhed, såsom ens smartphone, som derefter videresender information til en cloudtjeneste. Dataene er derefter tilgængelige for en ekstern part, såsom enhedsproducenten eller en læge. Denne konstellation af hardware og software, fysiske og logiske kommunikationsveje og organisatoriske grænser introducerer mange lag af kompleksitet, der hver især er modtagelige for fejl, forringelse, kompromittering og angreb.

Der har været bestræbelser på at katalogisere de sårbare evner opdaget i medicinsk udstyr. ICS-CERT (Industrial Control Systems Cyber Emergency Readiness Team), en afdeling af Department of Homeland Security, udsteder trusselsrådgivning for medicinsk udstyr. Medcrypt, en nonprofitorganisation inden for sundhedsvæsenet, vedligeholder et online dokument, der viser hver af disse råd.10 Pr. juli 2019 havde den dokumenteret 144 unikke sårbarheder opdaget siden 2013,11 og antallet af sårbarheder stiger,12 som vist i figur 2. Vi forventer at se en kontinuerlig vækst i IoB-sårbarhedsrapporter, blot fordi sikkerhedsforskere begynder at undersøge dette spirende felt.

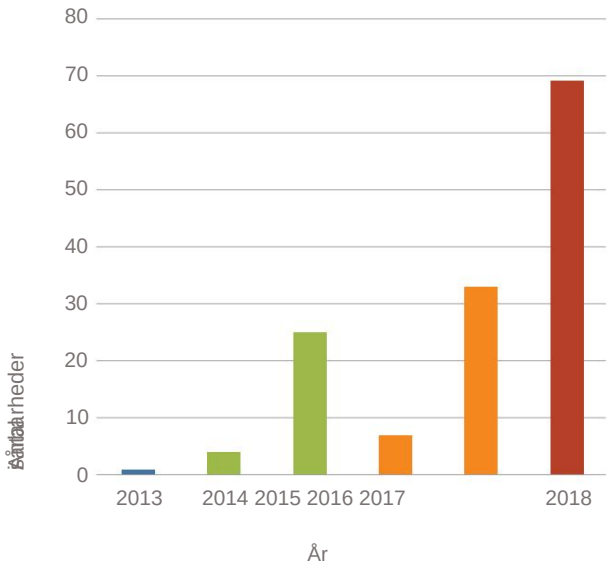
Af de sårbarheder, der findes i disse enheder, er størstedelen – 65 procent – fejl i brugergodkendelse og kodefejl. Brugergodkendelsesfejl kan give uautoriserede brugere adgang til og tilknytte data (f.eks. kompromittere enhedens fortrolighed). Kodefejl refererer til softwarefejl, der kan give en ondsindet bruger mulighed for at krænke systemets fortrolighed, integritet eller tilgængelighed. For eksempel kan en hacker få enheden til at dele data med uautoriserede brugere, manipulere dataene, så enheden opfører sig forkert, eller blot få enheden til at stoppe med at virke.

IoB-enheder står over for adskillige andre unikke sikkerhedsproblemer. Konventionelle anbefalinger til cybersikkerhed

Machine Translated by Google

FIGUR 2

Sårbarheder i medicinsk udstyr, efter år



KILDE: ICS-CERT trusselsadvarsler. ICS-CERT (Industrial Control Systems Cyber Emergency Readiness Team), en afdeling af Department of Homeland Security, udsteder trusselsadvarsler for medicinsk udstyr.

omfatte programrettelser (f.eks. installation af ny kode for at rette fejlbehæftet kode), anvendelse af afhjælpende foranstaltninger (f.eks. deaktivering af den berørte tjeneste eller softwarekomponent) og anvendelse af yderligere sikkerhedskontroller oven på den sårbare komponent for at maskere eller på anden måde blokere ethvert indgående angreb. I tilfælde af personlige sundhedsanordninger, der kan være implanteret i en persons krop, som kræver 24-timers tilgængelighed eller muligvis ikke kan bruges på nogen praktisk måde (for eksempel hvis patienten bor i et fjerntliggende område eller ikke kan besøge et sundhedscenter), er sådanne afhjælpende foranstaltninger muligvis ikke gennemførlige eller endda mulige.

Ud over cybersikkerheden på selve enhederne skal de datalagre, der lagrer brugerdata, også have tilstrækkelige sikkerheds-, software- og sikkerhedskontroller på plads. Hvis ikke, kan brugerne være i fare, som illustreret af den hurtige implementering af elektroniske patientjournaler. 21st Century Cures Act fra 2016 skulle løse vanskeligheder med implementeringen af elektroniske patientjournaler ved at forbedre interoperabiliteten mellem sundhedsinformationssystemer og patienters adgang til data. På trods af denne lovgivning har elektroniske patientjournaler, som i vid udstrækning havde til formål at afhjælpe medicinske fejl, været involveret i tusindvis af patientdødsfald, skader eller næsten-ulykker på grund af software. fejl, brugerfejl eller andre problemer (Schulte og Fry, 2019a).

Der kan også være kritiske afvejninger mellem sikkerhed og brugervenlighed for IoB-enheder. Overvej for eksempel en tilsluttet insulinpumpe. Bedste praksis for sikkerhed foreslår, at adgang til enheden begrænses til kun dem med den rette tilladelse til at frigive eller ændre injektionerne, noget der ofte gøres via brugernavne og adgangskoder eller via biometrisk login. En patient i insulinchok vil dog sandsynligvis ikke have tid eller mentale evner til at indtaste sine legitimationsoplysninger i enheden. Men brugervenlighed kan resultere i genveje til cybersikkerhed, og sådanne genveje kan true privatlivets fred.

Data- og privatlivsrisici

Data driver de algoritmer, der leverer målrettede annoncer, vurderer kredit- eller anden risiko og driver en stor del af internetøkonomien. IoB-enheder indsamler og lagrer meget personlige data, uden tvivl mere intime end nogen anden type brugerinformation, og derfor er der mange risici for privatlivets fred og fortrolighed. Oplysninger om brugernes opholdssted, kropsfunktioner, hvad de ser, hører og endda tænker, kan registreres og lagres.

Der er mange uafklarede spørgsmål om, hvem der har myndighed til at bruge data indsamlet af IoB-enheder, og på hvilken måde. For eksempel er der spørgsmål om, hvad retshåndhævende myndigheder kan gøre med IoB-oplysninger, og om en sådan brug er en overtrædelse af urimelige regler Beskyttelse mod ransagning og beslaglæggelse eller selvinkriminering garanteret af det 4. og 5. tillæg til den amerikanske forfatning. Medicinske oplysninger, såsom pacemakerdata, er allerede blevet brugt til at sigte folk for forbrydelser (Wootson, 2017). Der er blevet rejst bekymring over, hvordan politiet bruger data, der administreres af statsejede og -drevne datafusionscentre, som aggregerer og analyserer personoplysninger, herunder sundhedsdata, fra flere offentlige og private kilder (Haskins, 2019). Ifølge analysen af et fusionscenters brugermanual er oplysninger fra forskellige kilder "aggregeret og syntetiseret på en måde, der giver retshåndhævelse næsten alvidende viden om enhver mistænkt, de beslutter at overvåge".

(Haskins, 2019). Andre lande kan have lignende adgang til folks personlige oplysninger og samarbejde med USA i gensidighed (gensidig udveksling) af

Machine Translated by Google

data (US Immigration and Customs Enforcement, udateret).

Dataindsamling kan true IoB-brugeres privatliv, hvis der ikke er sikkerhedsforanstaltninger på plads til at beskytte mod misbrug. Selve indsamlingsprocessen, herunder hvilke data der indsamles, hvor ofte, om der er indhentet informeret samtykke (især i sårbare befolkningsgrupper såsom mindreårige eller fængslede personer), og om brugeren kan vælge at stoppe dataindsamlingen eller videresalget når som helst, kan udgøre en iboende risiko for privatlivets fred.

IoB-forbrugere synes at have accepteret behovet for at give deres data til udviklere eller andre for at bruge et IoB-produkt. Det er dog ikke klart, om forbrugerne har gået videre med fuldstændig viden om, hvordan deres data indsamles og kan bruges. En undersøgelse af CPAP-maskiner (Continuous Positive Airway Pressure), der bruges af personer med søvnapnø, viste, at patientdata blev sendt til forsikringsselskaber uden brugernes viden for at overvåge deres overholdelse (Allen, 2018a). Hvis patienterne ikke brugte CPAP-maskinen i den krævede periode, nægtede forsikringsselskabet at dække omkostningerne.

Information, der afslører usunde livsstilsvaner, kan allerede have resulteret i højere sundhedsforsikringspræmier for nogle mennesker (Allen, 2018b).
En stigning i antallet af IoB-enheder kan eskalere denne tendens med at kombinere sundhedsdata med andre personlige oplysninger, indsamlet af datamæglere – virksomheder, der ikke har nogen direkte relation til forbrugerne, men køber og sælger deres personlige oplysninger – for at øge præmier eller begrænse adgangen til pleje.

Der er spørgsmålet om iboende rettigheder, som en bruger kan være berettiget til. For eksempel, bør en bruger have ret til at fravælge enten visse typer dataindsamling eller lagring? Bør USA implementere en ret til at blive glemt for dem, der anmoder om sletning af deres data?13 Kritikere argumenterer for, at retten til at blive glemt kan krænke ytringsfriheden (Bowcott, 2018), give mulighed for ufuldstændige offentlige registre ("The Case Against a Right to Be Forgotten," 2018) eller give mulighed for, at historien omskrives af autoritære regimer (Swearingen, 2019).
Et andet spørgsmål er en posthum ret til privatliv, dvs. når en person dør, skal dataene så slettes, eller skal de være tilgængelige for nærmeste pårørende?14 Dette kan være et særligt følsomt spørgsmål problem i tilfælde af selvmord, eutanasi eller fosterovervågning.

Derudover kan fortolkning af IoB-data og algoritmiske output, der er afhængige af disse data, være forudindtaget eller på anden måde skadelig for brugeren, især hvis der er begrænset gennemsigtighed i disse processer (Osoba og Welser, 2017).

Der er også bekymringer om dataudholdenhed – det vil sige, at resultater fra et genetisk testkit eller brugen af en bestemt medicinsk enhed fra IoB kan identificere en person som bærer af en genetisk sygdom, der kan overføres til hans eller hendes børn, hvilket en dag kan resultere i, at disse børn nægtes visse forsikringer eller andre ydelser (Klitzman, 2012).

Endelig er der endnu ingen juridiske normer for, hvem der ejer de data, der genereres af en given IoB-enhed – brugeren, producenten, sundhedsudbyderen?
Dataejerskab har længe været et problem inden for sundhedsvæsenet (Meingast, Roosta og Sastry, 2006). Virksomhedsrådgivningsfirmaer undersøger, hvordan IoT-data bedst kan tjene penge på at generere penge (Deichmann et al., 2016; Russo og Albert, 2018). Politikker, der regulerer salg af brugeroplysninger til tredjeparts datamæglere, eller som regulerer, hvordan datamæglere fungerer, er i sin vorden, hvis de overhovedet eksisterer (MacMillan, 2019).

Etiske overvejelser

Mange af de risici, der tidligere er blevet diskuteret, kan betragtes som etiske, da de afspejler værdier, der er forbundet med sikkerhed og privatliv. Men vi skal også overveje de potentielt skadelige konsekvenser af IoB for andre værdier, der er vigtige for amerikanere, såsom lighed og personlig autonomi.

Ulige resultater

En af de lovede fordele ved IoB-teknologier er mindskede uligheder i sundhedsresultater i USA ved at gøre forebyggende og diagnostisk behandling billigere og lettere tilgængelig, men det er ikke klart, om disse teknologier vil mindske sundhedsomkostningerne eller være let tilgængelige for den brede befolkning.

Generelt har avancerede teknologier inden for sundhedsvæsenet bidraget til en stigning i de samlede omkostninger (Callahan, 2008). Uligheder på grund af adgangsbarrierer til digital sundhed og telehealth kan blive forværret

Machine Translated by Google

for dem uden pålidelig internetadgang (Gonzales, 2017). Mange af dem uden forsikring har ikke adgang til avancerede sundhedsteknologier. Selv for de forsikrede tilbyder udbydere muligvis ikke dækning af sofistikeret IoB, medmindre en cost-benefit-analyse viser, at sådanne enheder faktisk forbedrer kort- og langsigtede medicinske resultater i forhold til deres omkostninger. Dette vil kræve betydelig dokumentation, og det vil være vigtigt at vide, om disse fordele gælder på tværs af mange befolkningsgrupper (f.eks. ældre patienter, der muligvis er mindre teknologisk kyndige, befolkningsgrupper med lav socioøkonomisk status osv.).

Derudover er medicinske data sårbare over for inputbias, da typiske brugere af IoB-enheder er en selvselekterende gruppe. Der vides kun lidt om dem, der ikke bruger IoB-enheder – hvad enten det er af eget valg eller på grund af omkostninger eller andre adgangsbarrierer. Manglende repræsentativitet af sundhedsdata er et veldokumenteret problem, fordi de fleste kliniske data typisk indsamles om yngre, hvide, mandlige deltagere fra middel- og overklassen (Caplan og Friesen, 2017). På trods af at Revitalization Act fra 1993 kræver, at kliniske forsøg finansieret af National Institutes of Health skal omfatte kvinder og minoriteter, er der ikke gjort betydelige fremskridt (Geller et al., 2018, 2011). Storstilede sundhedsdata er, selvom de er hentet fra virkelige befolkningsgrupper, ikke immune over for inputbias – elektroniske patientjournaler og data om erstatningskrav involverer patienter, der er aktivt engageret i sundhedssystemer, hvilket resulterer i stikprøver, der har tendens til at være mere syge eller handicappede end den generelle befolkning (Agniel, Kohane og Weber, 2018; Verheij et al., 2018; Schneeweiss og Avorn, 2005). PGHD indsamlet fra forbrugere uden for klinikken kan omgå nogle af disse bias, men kræver andre overvejelser vedrørende stikprøveudtagning, som stort set er fraværende i tidlige studier.

Frihed fra IoB

Efterhånden som IoB bliver mere allestedsnærværende, kan der være et stigende fysisk eller psykologisk pres på dem, der ønsker at leve deres liv med minimal afhængighed af eller interaktion med disse enheder.

Nogle IoB-teknologier kan indsamle potentielt følsomme oplysninger ud over brugeren eller ejeren selv. For eksempel augmented reality-enheder eller "Smarte" høreimplantater er designet til at optage video og lyd. Dette kan give anledning til bekymring om privatlivets fred for personer, der ses eller høres af enhederne, men som ikke har givet samtykke til at få deres billeder eller stemmer indsamlet. Et eksempel på dette fænomen var reaktionen på Google Glass augmented reality-systemet, der skabte offentligt ramaskrig – tydeligt illustreret i "Stop the Cyborgs"-bevægelsen (Farivar, 2013). Brugen af ansigtsgenkendelsessystemer af retshåndhævende myndigheder har ført til kritik af, at systemerne er forudindtagede, men også at de bruges til at klassificere personer uden deres samtykke og med begrænset forståelse af, hvordan oplysningerne vil blive brugt (Axon AI and Policing Technology Ethics Board, 2019). Lignende kritik gælder for IoB med kameraer og andre værktøjer, der kan bruges til at optage eller identificere personer.

Nogle organisationer har søgt at bruge IoB til at administrere medarbejdere. Mens medarbejderbadges, der bruges til at få adgang til arbejdspladsen, ville blive betragtet som IoB-enheder, er der en skelnen mellem overvågning med passiv feedback (f.eks. bipper badgelæseren, og bygningsdøren låses op for at tillade adgang) og overvågning med feedback, der er netværksforbundet (f.eks. holder enheden konstant styr på brugerens opholdssted). Amazon har patenteret teknologier til et armbånd, der kan spore medarbejdernes adfærd, og som vibrerer for at give dem et skub til at opnå større produktivitet (Solon, 2018). Andre teknologier søger at identificere, hvornår medarbejdere er søvnige eller distraherede (Derousseau, 2017). Forskere er ved at skabe wearables, der hævder at spore en medarbejders præstation på arbejdspladsen (f.eks. mængden af tid brugt på arbejdet, pauser fra arbejdet, fysisk aktivitet og søvnniveau) med omkring 80 procents nøjagtighed (Holley, 2019). Disse muligheder kan gavne arbejdsgivere og gøre dem mere datadrevne og effektive (Knack et al., 2019), men de kan fremmedgøre medarbejdere og skade fastholdelsen af medarbejdere, hvis medarbejderne opfatter dem som påtrængende og unødvendige.

Tvungen implementering af IoB-teknologi kan være mest sandsynligvis vil forekomme inden for strafferetssystemet. Domstole, fængsler eller prøveløsladelseskontorer kan presse eller kræve, at folk bruger IoB-enheder. Mange jurisdiktioner bruger IoB-ankelarmbånd for at forhindre, at de, der afventer retssag, flygter. Selv hvis indsatte giver samtykke, er de muligvis ikke klar over potentielle risici. Man kan forestille sig IoB-behandlinger svarende til en digital aripiprazolbehandling.

Machine Translated by Google

pille, der bruges til at behandle psykiatriske lidelser, til at erstatte traditionel retsordret psykiatrisk behandling. Andre udvidede krav til dem, der er blevet arresteret eller dømt for forbrydelser, kan være at bruge IoB til at overvåge deres placering, helbred, alkohol- eller stofmisbrug eller andre indikatorer for opfattet socialt uønsket adfærd.

Kropslig autonomi og integritet

En anden etisk overvejelse vedrører brugernes rettigheder over teknologier, der er integreret i deres kroppe. Denne brugerret er dog potentielt i spænding med teknologiudvikleres forsøg på at bevare rettigheder over software og enheder. Et eksempel på denne spænding er slutbrugerlicensaftaler (EULA'er), som softwareudviklere bruger til at begrænse, hvad en bruger kan gøre ved software efter køb.

En EULA kan begrænse ændringer af software eller dens brug for at sikre den tilsigtede ydeevne eller beskytte intellektuel ejendomsret. Men når en enhed først er implanteret i en person, kan udviklerens fortsatte proprietære kontrol over enhederne blive problematisk (Matwyshyn, 2018; Matawyshyn, 2019; Atlantic Council, 2017; CPDP Conferences, 2018; Edinburgh Law School, 2018, kl. 26:28–28:08). Hvad hvis en udvikler f.eks. forsøger at gennemtvinge en aftale om en ændring af databrugspolitikker relateret til en enhed, der allerede er blevet (måske permanent) implanteret? Nogle vil argumentere for, at folk har en grundlæggende moralsk ret til kropslig autonomi, og denne ret bør give dem fuld kontrol over deres enheder som en forlængelse af deres kroppe.15 I det omfang brugerne ser enheden som en del af deres krop, kan de med rimelighed tro, at de har ret til at modsætte sig ændringer, der er pålagt af udvikleren. De kan også insistere på muligheden for at ændre enheden, som de finder passende.

Der er allerede eksempler på brugere, der "jailbreaker" eller hacker IoB-enheder for at forbedre deres funktionalitet (Brown, 2019; Hurley, 2014). Udviklere har dog frarådet disse ændringer med den begrundelse, at de kan påvirke enhedens funktionalitet negativt (Zhang, 2019).

Nogle typer af IoB er stort set uregulerede – for eksempel RFID-biochips eller sundhedssporingsteknologi. Men i fremtiden kan der være behov for at regulere vilkårene og betingelserne. hvorunder IoB-teknologier kan anvendes, og overveje beskyttelse af visse sårbare grupper, især for at sikre, at brugerne har rettigheder over teknologier i deres kroppe.

Styring af IoB-enheder og Information

Som med de fleste forbrugerprodukter i USA styres styringen af IoB-enheder gennem et kludetæppe af direkte og indirekte statslige og føderale agenturer, nonprofitorganisationer og forbrugerorganisationer. For eksempel sendes tilbagekaldelsesmeddelelser fra både FDA (FDA, 2018c) og Consumer Product Safety Commission (US Consumer Product Safety Commission, 2018). Federal Trade Commission (FTC) hjælper med at håndtere IoT-sikkerhed (FTC, 2015) og brud på sundhedsdata (FTC, 2010), og National Institute of Standards and Technology (NIST) påvirker både civil og statslig cybersikkerhed med aktiviteter relateret til IoT (NIST, 2019) og cyberfysiske systemer (NIST Cyber Physical Systems Public Working Group, 2016). I denne rapport udforsker vi ikke hver organisation i dybden, men giver et bredt overblik over de vigtigste styringsmæssige påvirkninger relateret til sikkerheden og privatlivets fred for IoB-enheder. Mere specifikt skelner vi mellem regler, der gælder for selve IoB-enheden, og regler, der gælder for de oplysninger, der indsamles, lagres eller transmitteres af enheden. Trods bestræbelserne på at regulere IoB undgår mange af disse enheder og de oplysninger, de indsamler, lovgivningsmæssig kontrol.

Styring af IoB-enheder

De primære enheder, der er ansvarlige for styring af IoB-enheder (vi behandler oplysninger indsamlet af IoB-enheder i det følgende afsnit) er FDA og det amerikanske handelsministerium.16

FDA's indsats

FDA, en del af det amerikanske sundhedsministerium, er ansvarlig for sikkerheden af medicinsk udstyr. I håb om at fremme innovation inden for digital sundhed har FDA udviklet et digitalt sundhedsdokument.

Machine Translated by Google

Innovationshandlingsplan. Imidlertid udelukker 21st Century Cures Act agenturet fra at have jurisdiktion over elektroniske patientjournaler. Tidligere FDA-chef Scott Gottlieb har opfordret Kongressen til at vedtage strammere regler for elektroniske patientjournaler og definere, hvornår en patients digitale journal kræver statsligt tilsyn (Schulte og Fry, 2019b).

For de IoB-teknologier, der er under FDA's tilsyn, fordi de er medicinsk udstyr, fremmer FDA cybersikkerhedsbeskyttelse gennem en tilgang, der fordeler ansvaret mellem forskellige interessenter. Agenturet samarbejder også med hackere og medicinsk udstyrsvirksomheder, f.eks. i DEFCON's Biohacking Village, for at finde og afsløre sårbarheder i medicinsk udstyr. FDA og private interessentgrupper har stået i spidsen for adskillige kampagner for bedre at vurdere og beskytte sikkerheden af implanteret og tilsluttet medicinsk udstyr. For eksempel har FDA siden 2013 afholdt adskillige offentlige workshops designet til at indhente og revidere vejledning, standarder og bedste praksis for cybersikkerhed inden for medicinsk udstyr (FDA, 2019c). Det har også udgivet vejledningsdokumenter før og efter markedet i et forsøg på at hjælpe enhedsproducenter med at forstå, hvordan de identificerer og afbøder cybersikkerhedstrusler og sårbarheder i deres produkter (FDA, 2018d; FDA, 2016; FDA, 2005). Disse dokumenter giver ikke-bindende vejledning i, hvordan en enhedsproducent kan opfylde FDA's regler for patientsikkerhed.

FDA offentliggør også rådgivende meddelelser om kendte sårbarheder i kritisk medicinsk udstyr og understøtter en e-mail-distributionsliste, der advarer brugerne, når problemer bliver kendte (FDA, 2019a). Der er også etableret informationsdelingsindsatser med analysecentre for sundhedsinformationsdeling (H-ISAC) for at lette udvekslingen af cybersikkerhedsrelaterede oplysninger mellem sundhedsudbydere og producenter. Disse to indsatser bidrager til at fremme informationsbevidsthed og gennemsigtighed for forbrugere og andre fagfolk og kan på lang sigt bidrage til at forbedre den samlede sikkerhed for disse enheder, selvom der endnu ikke er beviser for dette.

Derudover samarbejder FDA med MITRE Corporation til at udvikle et scoringssystem designet til at rangere alvorligheden af softwaresårbarheder i medicinsk udstyr (Chase og Coley, 2019). Selvom der allerede findes en branchestandard for scoring softwaresårbarheder i mere traditionelle computersystemer (se Common Vulnerability Scoring System SIG, udateret), det er et stumt instrument og adresserer ikke på passende vis de potentielle sikkerheds- eller sundhedsmæssige konsekvenser for en patient, hvis medicinske udstyr er hacket. Dette projekt vil sikre, at producenter og plejepersonale mere effektivt kan vurdere og prioritere risikoen for sårbarheder.

Selvom FDA gør fremskridt inden for cybersikkerhed Af hensyn til sikkerheden af medicinsk udstyr falder mange IoB-enheder, især dem, der er tilgængelige til forbrugerbrug, ikke under FDA's jurisdiktion.

Andre indsatser

Embedsmænd fra føderale og statslige myndigheder er begyndt at håndtere cybersikkerhedsrisici forbundet med IoT, som ligger uden for FDA's tilsyn, men der er få love, der pålægger bedste praksis for cybersikkerhed. Californien er den første stat, der vedtager en IoT-sikkerhedslov, SB-327, som trådte i kraft i januar 2020. Den californiske lov kræver, at en "producent af en tilsluttet enhed ... udstyrer enheden med en eller flere rimelige sikkerhedsfunktioner, der er passende for enhedens art og funktion." For eksempel specificerer den, at IoT-enheder ikke må have generiske standardadgangskoder.
Andre stater har debatteret lovgivning om IoT-sikkerhed, men har ikke vedtaget lovforslag. I marts 2019 genindførte en tværpolitisk gruppe af amerikanske senatorer Internet of Things Cybersecurity Improvement Act fra 2019, som forsøger at forbedre sikkerheden ved at dokumentere bedste praksis for udvikling, administration og patching af IoT-enheder og anbefaler, hvordan den amerikanske regering bedst kan anvende disse praksisser (Goodloe og Nandaraj Gallo, 2019). Dette lovforslag, som følger op på tidligere mislykket lovgivning, vil pålægge specifikke cybersikkerhedsstandarder for IoT-enheder, der købes af føderale agenturer, i håb om, at producenter frivilligt vil indføre disse til det kommercielle marked.

En væsentlig komponent i bestræbelserne på at styre nye teknologier er offentlig-private partnerskaber. For eksempel samarbejder NIST med offentlige og private partnere for at udvikle bedste praksis og retningslinjer, såsom sin cybersikkerhedsramme til håndtering af cyberrisiko. Medical Device Innovation Consortium (MDIC), et offentlig-privat partnerskab

Machine Translated by Google

mellem regeringen og interessenter i industrien, har kæmpet for at fremme en mere samarbejdsorienteret industridynamik, hvor forskere kan afsløre sårbarheder i disse medicinske anordninger uden frygt for civilretligt ansvar eller strafferetlig forfølgelse (MDIC, 2018).17 Fra midten af 2019 havde mere end 20 organisationer etableret sådanne programmer (I Am the Cavalry, udateret)

Ud over topstyrede indsatser for cybersikkerhedsstyring har adskillige græsrodsforkæmpere forsøgt at fremme bedste praksis inden for cybersikkerhed inden for forbundne medicinske apparater. For eksempel har den ikke-statslige organisation I Am the Cavalry udarbejdet det, de kalder en hippokratisk ed for forbundne medicinske apparater, med fem frivillige principper, som sundhedsudbydere og udstyrsproducenter bør vedtage for bedre at beskytte patienternes sikkerhed (Woods, Coravos og Corman, 2019).

Eden vedrører at sikre, at enheder og de oplysninger, der er indeholdt på enhederne, er modstandsdygtige over for indtrængen, kompromittering, manipulation og uautoriseret videregivelse, og at opdateringer og andre rettelser vil være hurtige og effektive.

Styring af IoB-data

Ligesom med IoB-enheder er der ingen enkelt enhed, der fører tilsyn med IoB-data. Tabel 5 opsummerer nogle af de primære enheder og deres ansvarsområder, selvom den overordnede regulering af privatlivets fred for personlige oplysninger er fragmenteret på tværs af mange statslige og føderale agenturer.18

Beskyttelse af medicinske oplysninger er reguleret ved på føderalt niveau, delvist af HIPAA. I mangel af anden føderal databeskyttelseslovgivning udgør HIPAA den primære ramme for beskyttelse af IoB-relaterede data. HIPAA-regel om meddelelse om brud på betingelserne, 45 CFR §§ 164.400-414, kræver specifikt, at HIPAA-dækkede enheder (sundhedsudbydere, sundhedsplaner og clearinghouses for sundhedsvæsenet) underretter berørte personer, når deres personlige helbredsoplysninger er blevet tilgået eller videregivet på en upassende måde, f.eks. når en hospitalsansat ser en patients journal, eller når en medicinsk database mistes eller bliver stjålet. Formålet med forordningen er at holde hospitaler og behandlere ansvarlige for mangler i datasikkerhedspraksis og give berørte personer mulighed for at overvåge deres økonomiske oplysninger og medicinske journaler nøje for at forhindre økonomisk eller medicinsk identitetstyveri.19 HIPAA dækker dog ikke ikke-medicinske sundhedsoplysninger eller biometriske oplysninger – faktisk dækker den ikke de fleste af de data, der indsamles af forbrugernes IoB-enheder.

FTC hjælper med at sikre datasikkerhed og forbrugernes privatliv gennem retssager anlagt af Bureau of Consumer Protection i henhold til afsnit 5(a) i FTC-loven, som fastslår, at "urimelige eller vildledende handlinger eller praksisser i eller som påvirker handel ... erklæres ... ulovlige." (15 USC Sec. 45[a][1]). Dette giver FTC beføjelse til at anlægge retssager mod virksomheder, der påviser en væsentlig mangel på datasikkerhed eller privatliv, eller som er vildledende om den måde, de bruger data på. I betragtning af sin tilsynsrolle udviklede FTC Mobile Health Apps Interactive Tool, en tjekliste designet til at hjælpe udviklere med at forstå

TABEL 5

Udvalgte ledelsesansvar for IoB-data

Agentur eller organisation	Ansvar
Det amerikanske sundhedsministeriums kontor for borgerrettigheder	Håndhæver loven om overførbarhed og regnskabsføring af sundhedsforsikringer (HIPAA)
Det amerikanske sundhedsministeriums kontor for den nationale koordinator for sundhedsinformationsteknologi	Koordinerer indsatsen for at sikre interoperabilitet mellem sundhedsoplysninger, herunder elektroniske patientjournaler
Den amerikanske føderale handelskommission (FTC)	Håndhæver datasikkerhed og forbrugernes privatliv gennem Bureau of Forbrugerbeskyttelse
Californiens justitsminister	Håndhæver Californiens lov om forbrugerbeskyttelse (CCPA)
Tilsynsmyndigheder i hver EU-medlemsstat	Håndhæv GDPR for at beskytte personoplysninger for EU-borgere

Machine Translated by Google

hvilke love der kan gælde for deres produkter. FTC har anlagt sag mod sociale medier og andre teknologivirksomheder, men vi fandt kun få eksempler på FTC-sager mod IoB-udviklere.20

Datamæglere er stort set uregulerede, men nogle Juridiske eksperter opfordrer til politikker, der beskytter forbrugerne. Data Broker Accountability and Transparency Act blev introduceret til Kongressen i 2017, men fik ingen medvind. I juni 2019 anbefalede 43 statsadvokater et nyt blik på en
FTC's anbefaling fra 2014 om, at Kongressen skulle oprette et føderalt register over alle datamæglere i landet (National Association of Attorneys General, 2019). Vermont blev den første stat til at vedtage en lov (Vermont Pub. LH764 [Act 171]), der regulerede datamæglere, som trådte i kraft den 1. januar 2019.
Loven kræver, at datamæglere registrerer sig i en offentlig database, specificerer de oplysninger, som en kunde ikke kan fravælge, forklarer muligheder for, hvad kunden kan fravælge, og angiver, om der er sket et databrud inden for det seneste år. Fra juli 2019 er Vermont den eneste stat, der har vedtaget politikker, der gør datamæglernes aktivitet mere gennemsigtig.

Da USA ikke har nogen føderal lov om databeskyttelse, har staterne indført et kludetæppe af love og regler, der gælder for beboernes personoplysninger, hvoraf nogle inkluderer oplysninger relateret til IoB. Disse love varierer meget på tværs af stater med hensyn til de typer af oplysninger, der beskyttes, og tilgængelige klagemuligheder, men overordnet set søger de at beskytte fortroligheden af forbrugeroplysninger og sikre, at patienter kan få adgang til oplysningerne efter anmodning, eller at sikre, at personlige sundhedsoplysninger kun bruges eller deles med patientens godkendelse (Smith, 2013).

Hver amerikansk stat har en lov, der kræver, at private Virksomheder og offentlige myndigheder underretter enkeltpersoner, når deres personlige oplysninger er blevet tilgået eller videregivet på en uautoriseret måde, f.eks. gennem et databrud ("Security Breach Notification Laws", 2018). Selvom der er en vis variation med hensyn til betingelserne for underretning, undtagelser og sanktioner, er underretning blevet en af de vigtigste håndhævelsesmekanismer til at forstå og håndtere databrud. Pr. 1. juli 2019 havde 16 stater vedtaget love, der eksplicit dækker ikke-medicinske biometriske oplysninger i deres regler om databrud, selvom hver stat varierer i sin definition af biometri (baseret på Hennessy et al., 2019). Wisconsin er den eneste stat, der inkluderer DNA i sin lov om offentliggørelse af brud på datasikkerheden som en specifik beskyttet datatype, der er forskellig fra biometriske oplysninger (Wis. Stat. §134.98).

Illinois og Texas har vedtaget love, der regulerer om enheder kan indfange eller indsamle biometriske oplysninger til kommercielle formål uden samtykke, begrænset til "en nethinde- eller iris-scanning, fingeraftryk, stemmeaftryk eller optagelse af hånd- eller ansigtsgeometri" (Illinois Biometric Information Privacy Act, 2019; Texas Business and Commerce Code, Title 11, Subtitle A, Chapter 503, 2009).

Washington vedtog en lov, der trådte i kraft den 1. marts 2020, som kræver, at enheder oplyser om indsamling og lagring af biometriske data til kommercielle formål, indhenter samtykke eller udvikler foranstaltninger, der forbyder efterfølgende salg af disse oplysninger, hvor biometriske data omfatter "unikke biologiske mønstre eller karakteristika ... der bruges til at identificere en specifik person".
(Revideret Washington-lovbog kapitel 19.375, 2019).
Mindst et dusin andre stater har foreslået lignende lovgivning om biometrisk privatliv.

CCPA, der trådte i kraft den 1. januar 2020, har til formål at forbedre kundernes privatliv ved at give enkeltpersoner ret til at vide, hvilke oplysninger der indsamles om dem, formålene med denne indsamling, og hvor disse oplysninger deles. Kunder kan også fravælge, at en virksomhed sælger deres personoplysninger, og loven kræver, at virksomheder, der indsamler personoplysninger, sletter optegnelsen efter anmodning fra forbrugeren.
Personoplysninger i CCPA er defineret bredt og omfatter biometriske oplysninger, geolokationsdata og endda slutninger fra de data, der bruges til at opbygge en psykologisk profil af personen. Mindst otte andre stater har udarbejdet lignende databeskyttelseslove.

Den Europæiske Union har vedtaget GDPR, en samling af regler, der er designet til at beskytte personlige oplysninger for EU-borgere, som også gælder for software- eller hardware-IoB-udviklere og -producenter. GDPR kræver, at brugerne giver informeret samtykke, før deres personlige oplysninger indsamles, og at deres oplysninger beskyttes på et niveau, der er passende i forhold til risikoniveauet (skadeniveauet) for brugeren. Derudover giver GDPR EU-borgere rettigheder over de data, som virksomheder indsamler fra dem, herunder retten til at få adgang til, slette eller overføre dataene til andre dataansvarlige. Lovgivere i

Machine Translated by Google

Kongressen arbejder på regler, der ville sætte en amerikansk standard for forbrugerdatabeskyttelse og retsmidler svarende til GDPR eller CCPA, men har pr. juni 2019 ikke vedtaget nogen politikker (Ratnam, 2019).

Manglen på ensartethed i IoB-lovgivningen på tværs af stater og mellem statsligt og føderalt niveau muliggør potentielt huller i lovgivningen og udfordringer med håndhævelsen.
Som på mange områder har den hurtige udvikling inden for IoB-teknologier overhalet udviklingen af politikker til at håndtere risiciene. Sådanne politikker vil kræve en fin navigation mellem yderpunkterne af underregulering, der ikke formår at afbøde risici, og overregulering, der hæmmer samfundsmæssigt gavnlig innovation eller forbrugeradoption. Det vil være bydende nødvendigt at finde en balance mellem innovation og regulering for at beskytte forbrugerne, samtidig med at fordelene opretholdes og USA holdes i spidsen for dette konkurrenceprægede felt.

Ser frem til at modtage adressen Risiko

Denne rapport har udforsket det komplekse og udviklende IoB-økosystem og identificeret en række potentielle fordele og risici. En lang række offentlige og ikke-offentlige interessenter spiller en rolle i dette økosystem, og hver interessent kan tage konstruktive skridt i retning af at håndtere risikoområder. Hvis disse risici ikke håndteres tilstrækkeligt, vil de medicinske, sundhedsmæssige og andre fordele ved IoB ikke blive fuldt ud realiseret.

Fremme af national sikkerhed

IoB-enheder indsamler følsomme personlige oplysninger, der kan bruges af udenlandske fjender til at udføre spionage eller forstyrre værdier og praksisser, der er vigtige for amerikanere. Kongressen og den udøvende magt har specifikke roller i at beskytte mod disse risici. Disse bestræbelser skal række ud over traditionelle nationale sikkerhedspolitikker for også at håndtere den nye dynamik forbundet med den udbredte brug af IoB og trusler fra fjender.

Havde begivenhederne, der involverede Strava eller vicepræsident Hvis Cheney havde været anderledes, kunne konsekvenserne have været enorme. Regeringsafdelinger kan tage disse hændelser som en lære af risiciene.

præsenteret af IoB og udvikle passende svar, ligesom Forsvarsministeriet gjorde. For eksempel kunne der udvikles retningslinjer for brugen af IoB til højtstående embedsmænd.

Efterhånden som brugen af IoB spreder sig i autoritære regimer, Det amerikanske handelsministerium kan sætte udenlandske IoB-virksomheder på sin "Entity List" og dermed forhindre dem i at handle med amerikanere, hvis disse udenlandske virksomheder er impliceret i krænkelser af menneskerettighederne.
Dette er blevet gjort mod kinesiske enheder, der undertrykker uighurer og andre minoritetsgrupper (Moss, 2019). CFIUS bør også fortsætte med at overvåge og undersøge udenlandske investeringer i og opkøb af amerikanske virksomheder, især dem, der behandler følsomme IoB-data om amerikanere.

Trusler mod amerikanske kommunikationsnetværk kan forekomme stige i takt med at IoB vinder popularitet, så i takt med at 5G-, Wi-Fi 6- og satellitinternetstandarder udrulles, bør den føderale regering proaktivt finansiere undersøgelser og samarbejde med eksperter om at udvikle sikkerhedsregler.

Fremme af cybersikkerhed

Alle netværksforbundne teknologier indebærer en cybersikkerhedsrisiko, men følsomheden af IoB-information og de potentielle medicinske og sundhedsmæssige konsekvenser af at forstyrre eller manipulere IoB er af akut bekymring.
Som tidligere beskrevet har interessenter søgt at fremme bedste praksis inden for cybersikkerhed for dele af IoB-økosystemet, herunder gennem indsatser ledet af FDA, det amerikanske ministerium for indenlandsk sikkerhed, handelsministeriet og ikke-statslige organisationer. Imidlertid er ikke alle IoB-enheder underlagt FDA's tilsyn, og den føderale regering har heller ikke indført bindende cybersikkerhedsstandarder for IoB.

Der er muligheder for at gøre mere for at fremme cybersikkerhed inden for IoB.

Den føderale regering, herunder de udøvende organer og Kongressen, kan først overveje, hvordan man implementerer en risikostyringstilgang, der etablerer bedste praksis og standarder for cybersikkerhed for hele spektret af IoB-produkter. For eksempel kunne en IoB-specifik ramme modelleres efter NIST's cybersikkerhedsramme. Denne indsats vil være mest effektiv, hvis den udføres i samråd med

brancheorganisationer og læger for at sikre, at regeringen fuldt ud forstår

Machine Translated by Google

Teknologien og de dertilhørende omkostninger – herunder hindringer for innovation – ved cybersikkerhedsforslag.
Det er vigtigt at bemærke, at en tilgang, der tager højde for hele spektret af IoB, vil gå ud over FDA's eksisterende indsats og også omfatte sundhedsudstyr til forbrugere og elektroniske patientjournaler. Som en del af denne risikostyringstilgang vil det være vigtigt at overveje, hvordan man kan tilskynde til hurtigere udfasning af ældre medicinsk udstyr med dårlig cybersikkerhed, der allerede er i vid udstrækning anvendes. Et muligt skridt ville være at udvikle og administrere cybersikkerhedscertificeringer for IoB (svarende til et Energy Star-mærke eller en næringsværdimærkning), der i stedet for at kræve en bestemt minimal cybersikkerhedsstandard ville give forbrugerne større bevidsthed om produkters cybersikkerhed og derved muliggøre markedsincitamenter for producenter af IoB-udstyr til at følge specifikke retningslinjer for cybersikkerhed ("Sådan opnår et produkt ENERGY STAR-mærket", udateret).
Dette forslag bør sammen med andre undersøges i samarbejde med interessenter.

Ud over offentlige aktører, sundhedsvæsenet Udbydere skal overveje implikationerne for cybersikkerhed, når de anbefaler eller bruger IoB. Som en start skal medicinske miljøer fortsætte med at udnytte cybersikkerhedsekspertise – for eksempel ved at bruge offentliggjorte retningslinjer, der rådgiver om, hvordan man opbygger en cyberarbejdsstyrke inden for sundhedsvæsenet.21 Udbydere kan også forpligte sig til at overholde den hippokratiske ed for forbundne medicinske enheder, skrevet af græsrodsorganisationen I Am The Cavalry, som opfordrer sundhedsudbydere og interessenter til at anerkende vigtigheden af cybersikkerhed for patienter.

Tilsvarende skal IoB-udviklere være mere opmærksomme til cybersikkerhed – for eksempel ved at følge FDA's retningslinjer for cybersikkerhed (selvom enheden ikke er medicinsk udstyr) og ved at integrere cybersikkerheds- og privatlivshensyn fra begyndelsen af produktudviklingen. Enhedsproducenter bør ofte teste software for sårbarheder – herunder ved hjælp af programmer til afsløring af sårbarheder – og udtænke metoder, som brugerne kan bruge til at opdatere software. Derudover skal enhedsproducenter etablere politikker for at underrette og beskytte forbrugeren, hvis der opstår cybersikkerheds- eller andre problemer (f.eks. hvis enheden skal opdateres, eller hvis den ikke længere understøttes af producenten). Denne indsats skal overveje og adressere de unikke udfordringer ved cybersikkerhed for IoB – for eksempel udfordringen med at patche enheder, der er implanteret og ikke let kan tilbagekaldes. Andre bedste praksisser inden for cybersikkerhed for IoB omfatter trusselsmodellering, datalagringsstandarder og opbevaring af softwarekildekode, der kan gennemgås af uafhængige cybersikkerhedsforskere.

Sikring af privatlivets fred

USA har ikke en omfattende føderal databeskyttelseslovgivning, og mange af de data, der indsamles af IoB, er ikke reguleret af gældende statslovgivning. Dette er komplekse politikområder, og IoB's omfang er bredt, så det er usandsynligt, at der findes en enkelt politik, der kan håndtere dem alle.
For at imødegå risikoen for privatlivets fred fra IoB-enheder bør Kongressen overveje at etablere føderale standarder for datatransparens og beskyttelse af data, der indsamles fra dem. Som det ser ud nu, har forbrugerne begrænset mulighed for at identificere, hvem der opbevarer deres intime sundheds- og andre data, og hvordan disse data bliver brugt – så som udgangspunkt for regulering kan offentlige enheder tage skridt til at sikre større gennemsigtighed omkring dataindsamlingspraksis. Efterhånden som konsekvenserne af reguleringer som GDPR og CCPA viser sig, kan Kongressen tage ved lære af både deres succeser og fiaskoer og overveje hvordan man giver IoB-brugere rettigheder over deres personlige oplysninger, herunder retten til at fravælge indsamling. Forbunds- og statslige myndigheder kan også overveje regler for datamæglere, begrænsninger på, hvem der kan indsamle data, hvordan sådanne oplysninger bruges, om de sælges til tredjeparter og så videre.

Der er også en rolle for den føderale regering i at harmonisere kludetæppet af statslige love vedrørende databrud og sundhedsoplysninger gennem en føderal standard for underretning om databrud.

Regeringen kan fremme og finansiere uafhængig forskning i nye problemstillinger som dataudholdenhed, privatlivets fred efter døden og retten til at blive glemt i forbindelse med IoB-data. Der skal også fastsættes regler for, hvordan forsikringsselskaber, arbejdsgivere eller andre har tilladelse til at bruge IoB-data.

Myndigheder og ressourcer til privatlivets fred i forbindelse med sundheds- og IoB-data deles mellem en række offentlige organisationer, herunder FTC, NIST og Health and Human Services (som FDA er en del af). Kongressen skal beslutte, hvilken delmængde af disse der skal

Machine Translated by Google

Organisationer ville være bedst egnede til at håndhæve krænkelser af privatlivets fred og databeskyttelsespolitikker vedrørende IoB-enheder. Der kan være behov for at allokere yderligere ressourcer, så der er tilstrækkelig støtte til rådighed til at håndhæve reglerne, efterhånden som IoB-produkter bliver mere udbredte. For eksempel har FTC på nuværende tidspunkt kun 40 fuldtidsansatte dedikeret til databeskyttelse (sammenlignet med 500 i Storbritanniens databeskyttelsesmyndighed), og FTC's formand, Joseph Simons, har udtalt, at agenturet ikke har tilstrækkelige ressourcer til at øge sin håndhævelse af databeskyttelsesreglerne (Simons, 2019).

Øget bevidsthed

Den hurtige udvikling af IoB har skabt et miljø, hvor forbrugere ubevidst bruger IoB, og hvor der er forvirring og mangel på klarhed om dets fordele og potentielle etiske ulemper.

IoB-økosystemet er muligvis ikke så nyttigt for sundhedsudbydere eller forbrugere, som det måske ser ud til, i hvert fald ikke på kort sigt. For eksempel har nogle undersøgelser vist, at konstant sporing af biometrisk aktivitet via sundhedsapps, såsom søvntrackere, kan øge brugernes angst og forværre tilstande som søvnløshed (Baron et al., 2017; Zraick og Mervosh, 2019). Mange IoB-teknologier har endnu ikke udviklet et klinisk evidensgrundlag for langsigtede resultater.

Interessenter bliver nødt til at undersøge og udbrede information om de realistiske og pragmatiske fordele ved IoB, efterhånden som det bliver mere mainstream, og også hvor der sandsynligvis vil opstå skadevirkninger.

FTC spiller allerede en vigtig rolle i forhold til markedsføringen af IoB-teknologier,22 og der er muligheder for, at FTC kan spille en større rolle for at sikre, at markedsføringspåstande om forbedret velvære eller specifik sundhedsbehandling understøttes af passende beviser. FTC kan dog have brug for yderligere ressourcer til at håndtere den brede vifte af IoB-teknologier, der er kommet på markedet i de senere år, og yderligere personale med ekspertise inden for IoB vil være vigtigt for at sikre, at IoB-udviklernes påstande ikke er vildledende eller urimelige.

Der er også muligheder for at øge bevidstheden om de etiske implikationer af IoB, for eksempel gennem yderligere føderal eller fondsfinansiering af forskning relateret til uligheder forbundet med IoB-dataindsamling og sundhedspleje. Denne forskning kan også fokusere på, i hvilket omfang IoB krænker autonomi på arbejdspladsen eller på anden måde underminerer rimelige forventninger til anonymitet eller privatliv.

Forbunds- og statslige myndigheder kan også samarbejde med partnere om at udvikle retningslinjer for ansvarlig udvikling og markedsføring af IoB. Statslige myndigheder kan samarbejde med opinionsdannere på universiteter og andre institutioner for at udnytte ekspertise inden for IoB-relaterede politiske emner, såsom cybersikkerhed og digital sundhed.23 Disse typer partnerskaber mellem beslutningstagere og eksperter kan hjælpe med at identificere huller i reguleringssystemet, fremme innovation inden for teknologiudvikling og beskytte alle interessenter.

Selv uden en regulerende funktion kan IoB-udviklere være tydeligere over for forbrugerne om cybersikkerhedsrisici og databeskyttelsespraksisser forbundet med deres produkter. IoB-udviklere indsamler enorme mængder intime data, og de skal klart angive deres privatlivspolitikker og indhente informeret samtykke til deres indsamlingspraksis. Disse politikker bør tydeligt forklare, hvordan data vil blive beskyttet, hvordan disse data vil blive brugt, og med hvem de kan deles. Udviklere bør også uddanne offentligheden om de risici, der er forbundet med IoB-produkter.

Endelig skal patienter og forbrugere erkende risiciene ved IoB og overveje disse risici, når de beslutter sig for at bruge sådanne enheder. I mangel af nye regler bør forbrugerne være forsigtige og gå ud fra den antagelse, at når data er indsamlet af en IoB-enhed, vil forbrugeren sandsynligvis ikke have fuld kontrol over, hvordan disse data opbevares og bruges, og bør være forberedt på, at de potentielt kan blive brudt eller på anden måde deles bredt. I sidste ende skal forbrugerne være opmærksomme på, at deres intime data indsamles af enheder, der ikke nødvendigvis har forbrugernes bedste interesser i tankerne. Øget bevidsthed om IoB-økosystemet og dets risici er afgørende.

Machine Translated by Google

Noter

1 En definition af IoB, fremsat af Matwyshyn, er "menneskekroppens snigende afhængighed af software, hardware og internettet for centrale aspekter af deres funktionalitet" (The Internet of Bodies, 2018). Tre generationer af IoB er defineret: krops-ekstern, krops-intern og krops-sammensmeltet (Matwyshyn, 2019).

[2] Vi begrænser vores definition af IoB-enheder til teknologier, der kan knyttes til et individ, snarere end til teknologier, der er knyttet til træk, der er mere eller mindre universelle for alle mennesker, eller en bestemt sygdom. Derfor betragtes store genetiske sekvensdatabaser (såsom GenBank) ikke som IoB-data, og teknikker (såsom CRISPR), der muliggøres af sådanne databaser, betragtes ikke som IoB-teknologier.

3 FDA definerer medicinsk udstyr som følger (FDA, 2018a):

- et instrument, apparat, redskab, maskine, anordning, implantat, in vitro-reagens eller anden lignende eller relateret artikel, herunder en komponent eller tilbehør, som er: anerkendt i den officielle nationale formular, eller De Forenede Staters farmakopé eller ethvert tillæg til dem,
- beregnet til brug ved diagnosticering af sygdomme eller andre tilstande, eller ved helbredelse, lindring, behandling eller forebyggelse af sygdomme hos mennesker eller andre dyr, eller
- beregnet til at påvirke strukturen eller enhver funktion af menneskets eller andre dyrs krop, og som ikke opnår sine primære tilsigtede formål gennem kemisk virkning i eller på menneskets eller andre dyrs krop, og som ikke er afhængig af at blive metaboliseret for at opnå nogen af sine primære tilsigtede formål.

[4] Et koncept relateret til IoT og IoB er cyberfysiske systemer. Ifølge Networking and Information Technology Research and Development (NITRD) er cyberfysiske systemer "smarte netværkssystemer med indlejrede sensorer, processorer og aktuatorer, der er designet til at registrere og interagere med den fysiske verden (inklusive de menneskelige brugere)" (NITRD, 2015).

5 Der er adskillige yderligere termer, der ikke er beskrevet her, som relaterer sig til IoB – såsom teknologier til forbedring af mennesker, DIYbio (gør-det-selv-biologi), wetware (direkte forbindelser mellem hjerne og computer) og kvantificeret selv – som er en del af dette voksende felt af kropsforbundne teknologier.

[6] Vi definerer fritstående enheder som dem, der står og fungerer på egen hånd, fri for kontinuerlig kropslig tilknytning.

7 Den nye Wi-Fi 6-standard, også kaldet 802.11ax, er under udvikling og forventes endeligt godkendt i juni 2020 ("Official IEEE 802.11 Working Group Project Timelines," 2019).

8 En angrebsflade er mængden af alle potentielle indgangspunkter, der kan bruges til at angribe et system (Manadhata og Wing, 2010).

[9] Sikkerhedsrisiciene ved computerstyret medicinsk behandling er dog enheder dateres tilbage til mindst 1985 (Leveson, 1995).

10 Dette dokument er ikke offentligt tilgængeligt.

11 Dette er sandsynligvis en undervurdering af det faktiske antal kendte sårbarheder, fordi denne liste sandsynligvis ikke omfatter alle sårbarheder fra softwarebiblioteker, der er designet til andre produkter, men som bruges i disse systemer.

[12] Data fra 2019 var ikke inkluderet.

13 Retten til at blive glemt er en del af Den Europæiske Unions generelle forordning om databeskyttelse (GDPR), men fra juni 2019 kan den kun håndhæves inden for Den Europæiske Union.

14 I øjeblikket gælder den juridiske ret til privatliv for levende personer og ikke afdøde (Banta, 2016). HIPAA-privatlivsreglerne opretholdes i 50 år efter afdødes død (US Department of Health and Human Services, 2013).

15 Som argumenteret i en undersøgelse om etikken bag menneskelig forbedring, "skaber det en intim eller forstærket forbindelse med vores værktøjer at assimilere dem i vores person" (Allhoff et al., 2010).

16 Der findes adskillige andre organisationer, der har en fælles rolle i den overordnede sikkerhed for IoB- og IoT-enheder, såsom Consumer Product Safety Commission, men en fuldstændig diskussion af alle relevante organer ligger uden for dette arbejdes rammer.

17 Sikker offentliggørelse af softwaresårbarheder er en luksus, som forskere ikke altid har nydt godt af. Heldigvis er der en voksende bevægelse for at fremme en åben og gennemsigtig proces for forskeres underretning til leverandører.

18 En fuldstændig diskussion af regulering af privatlivets fred ligger uden for dette arbejdes rammer; se dog Mulligan, Freeman og Linebaugh (2019).

[19] Det er dog udokumenteret, om denne regel har forbedret datasikkerhedspraksis.

[20] Et eksempel er beskrevet i Morris (2017).

[21] Et eksempel er "Healthcare Industry Cybersecurity Work-force Guide" (Healthcare and Public Health Sector Coordinating Council, udateret). Et andet eksempel, der ikke specifikt er rettet mod sundhedsorganisationer, er NIST's "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework" (Nationalt initiativ for cybersecurity-uddannelse (NICE) Cybersecurity Workforce Framework). (Newhouse et al., 2017).

22 FTC er ikke den eneste organisation, der er involveret her; FDA regulerer for eksempel markedsføringen af medicinsk udstyr.

[23] For eksempel har Center for Body Computing ved University of Southern California indgået et partnerskab med Californiens guvernørs kontor for erhvervs- og økonomisk udvikling for at udvikle og formidle koncepter for cybersikkerhed inden for informationsteknologi inden for sundhedsvæsenet (University of Southern California Center for Body Computing, 2018).

Machine Translated by Google

Referencer

Agboola, Stephen, Kamal Jethwani, Kholoud Khateeb, Stephanie Moore og Joseph Kvedar, “Fjernovervågning af hjertesvigt: Evidens fra den retrospektive evaluering af et fjernovervågningsprogram i den virkelige verden,” Journal of Medical Internet Research, bind 17, nr. 4, 2015, s. e101.

Agniel, Denis, Isaac S. Kohane og Griffin M. Weber, “Skema i elektroniske patientjournaldata på grund af processer inden for sundhedssystemet: Retrospektiv observationsundersøgelse,” BMJ, bind 361, 2018, s. k1479.

Allen, Marshall, “Sundhedsforsikringsselskaber støvsuger detaljer om dig op – og det kan hæve dine priser,” ProPublica, 17. juli 2018a. Pr. 3. juli 2019: https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates

———, "Du slumrer, du taber: Forsikringsselskaber gør det gamle ordsprog bogstaveligt talt sandt," ProPublica, 21. november 2018b. Pr. 27. april, 2020: https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true

Allen-Graham, Judith, Lauren Mitchell, Natalie Heriot, Roksana Armani, David Langton, Michele Levinson, Alan Young, Julian A. Smith, Tom Kotsimbos og John W. Wilson, “Elektroniske patientjournaler og online patientjournaler: Et aktiv eller en passiv under de nuværende forhold?” Australian Health Review, bind 42, nr. 1, 2018, s. 59–65.

Allhoff, Fritz, Patrick Lin, James Moor og John Weckert, “Etik i menneskelig forbedring: 25 spørgsmål og svar,” Studier i etik, jura og teknologi, bind 4, nr. 1, 2010, s. Artikel-4.

Apple, “EKG-app og notifikation om uregelmæssig hjerterytme tilgængelig i dag på Apple Watch,” pressemeddelelse, 6. december 2018.

Appleby, Julie, “Et wake-up call om smarte senge og søvnapps, der indsamler dine data,” Time, 29. maj 2019. Pr. 27. april, 2020: https://time.com/5592792/a-wake-up-call-on-smart-beds-and-sleep-apps-that-collect-your-data/

Atlantic Council, Cyber Risk Thursday: Internet of Bodies, webcast, 21. september 2017. Pr. 27. april 2020: https://www.atlanticcouncil.org/unused/webcasts/cyber-risk-thursday-internet-of-bodies/

Axon AI og Policing Technology Ethics Board, første rapport fra Axon AI & Policing Technology Ethics Board, juni 2019. Pr. 27. april 2020: https://static1.squarespace.com/statisk/58a33e881b631bc60d4f8b31/t/5d13d7e1990c4f00014c0aeb/1561581540954/Axon_Etik_Bestyrelses_Første_Rapport.pdf

Baenen, Jeff, “Wisconsin-virksomhed holder 'chipfest' for mikrochiparbejdere,” Chicago Tribune, 2. august 2017. Pr. 27. april 2020: https://www.chicagotribune.com/business/blue-sky/ct-wisconsin-company-microchips-workers-20170801-story.html

Banta, Natalie M., Død og privatliv i den digitale tidsalder, North Carolina Law Review, bind 94, nr. 3, 2016, s. 927. Pr. 27. april 2020: https://scholarship.law.unc.edu/nclr/vol94/iss3/4/

Baron, Kelly Glazer, Sabra Abbott, Nancy Jao, Natalie Manalo og Rebecca Mullen, “Orthosomnia: Tager nogle patienter det kvantificerede selv for langt?” Journal of Clinical Sleep Medicine, bind 13, nr. 2, 2017, s. 351–354. Pr. 27. april 2020: http://jcsm.aasm.org/viewabstract.aspx?pid=30955

Bauerle Danzman, Sarah og Geoffrey Gertz, “Hvorfor er USA Tvinge et kinesisk firma til at sælge datingappen Grindr til homoseksuelle? Washington Post, 3. april 2019. Pr. 27. april 2020: https://www.washingtonpost.com/politics/2019/04/03/hvorfor-tvinger-os-kinesiske-firmaer-til-at-sælge-dating-app-til-bøsse-grindr/?noredirect=on&utm_term=.6ca317886ff3

Beardsley, Tod, “R7-2016-07: Flere sårbarheder i Animas OneTouch Ping-insulinpumpe,” Rapid7-blog, 2016. Pr. 27. april 2020: https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/

Bentley, Daniel, “Denne hospitalsseng kan redde liv,” Fortune, 20. marts 2018. Pr. 27. april 2020: https://fortune.com/2018/03/20/earlysense-hospital-bed/

Binnendijk, Annika, Robert Timothy Marler og Elizabeth M. Bartels, Hjerne-computer-grænseflader: Amerikanske militære anvendelser og implikationer, en indledende vurdering, Santa Monica, Californien: RAND Corporation, RR-2996-RC, udkommer snart.

Boughton, CK og R. Hovorka, “Er en kunstig bugspytkirtel (lukket kredsløbssystem) effektiv til type 1-diabetes?” Diabetic Medicine, bind 36, nr. 3, 2019, s. 279–286.

Bowcott, Owen, “'Retten til at blive glemt' kan true den globale ytringsfrihed, siger NGO'er,” The Guardian, 9. september 2018. Pr. 27. april 2020: https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos

Braveman, Paula, Catherine Cubbin, Susan Egerter, Sekai Chideya, Kristen Marchi, Marilyn Metzler og Samuel Posner, “Socioøkonomisk status i sundhedsforskning: Én størrelse passer ikke til alle,” Journal of the American Medical Association, bind 294, nr. 22, 2005, s. 2879–2888.

Brown, Dalvin, “Hacking Diabetes: Folk bryder ind i insulinpumper som et alternativ til forsinkede innovationer,” USA Today, 5. juni 2019. Pr. 27. april 2020: https://www.wired.com/2014/12/diabetes-patients-hacking-together-diy-bionic-pancreases/

Bryan-Low, Cassell, Colin Packham, David Lague, Steve Stecklow og Jack Stubbs, “At hæmme Huawei: Inde i USA” "Krig mod Kinas techgigant," Reuters, 21. maj 2019. Pr. 27. april 2020: https://www.reuters.com/investigates/special-report/huawei-usa-campaign/

Bushatz, Amy, “Army Udsteder FitBit-Remme i Test Fitness Program,” pressemeddelelse, Military.com, 22. oktober 2013. Pr. 27. april 2020: https://www.military.com/daily-news/2013/10/22/army-issues-fitbit-bands-in-test-fitness-program.html

Callahan, Daniel, Bioetikbriefingbog for journalister, beslutningstagere og kampagner: Sundhedsomkostninger og medicinsk teknologi, Garrison, NY: The Hastings Center, 2008. Pr. 27. april 2020: https://www.thehastingscenter.org/briefingbook/health-care-costs-and-medical-technology/

Caplan, Arthur L., og Phoebe Friesen, “Sundhedsforskelle og rekruttering til kliniske forsøg: Er der en pligt til at tweete?” PLoS Biology, bind 15, nr. 3, 2017, s. e2002040.

Machine Translated by Google

Center for Internetsikkerhed, “EI-ISAC Cybersecurity Spotlight” "CIA Triad," hjemmeside, udateret. Pr. 27. april 2020: https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/

Chase, Penny og Steve Christey Coley, “Rubrik for anvendelse af CVSS på medicinsk udstyr,” MITRE Corp., 16. januar 2019.

Chen, Xing, Babak Assadsangabi, York Hsiang og Kenichi Takahata, “Muliggørelse af angioplastik-klare 'smarte' stents til at detektere restenose og okklusion i stenten,” Advanced Science, bind 5, nr. 5, 2018, s. 1700560.

Clymo, Rob, “AI i bilen kan snart vide, om du har en god eller dårlig dag,” TechRadar, 4. oktober 2018. Pr. 27. april, 2020: https://www.techradar.com/news/in-car-ai-could-soon-know-if-youre-having-a-good-or-bad-day

Coates McCall, Iris, Chloe Lau, Nicole Minielly og Judy Illes, “At eje etisk innovation: Påstande om kommercielle bærbare hjerneteknologier,” Neuron, bind 102, nr. 4, 22. maj 2019, s. 728–31.

“Common Vulnerability Scoring System SIG,” hjemmeside, FIRST, Cary, NC, udateret. Pr. 27. april 2020: https://www.first.org/cvss/

Copp, Tara, “Fitbits og fitness-tracking-enheder forbudt for udsendte tropper,” Military Times, 6. august 2018. Pr. 27. april 2020: https://www.militarytimes.com/news/your-military/2018/08/06/enheder-og-apps-der-er-afhængige-af-geolokalisering-begrænset-for-udsendte-tropper/

CPDP-konferencer, “CPDP 2018: Internettet for (sårbare) "Bodies," YouTube-video, Computere, privatliv og databeskyttelse, 6. februar 2018. Pr. 28. april 2020: https://www.youtube.com/watch?v=10Rlk8uj-lo

Das, Ashok Kumar, Sherali Zeadally og Mohammad Wazid, “Lette godkendelsesprotokoller til bærbare enheder,” Computere og elektroteknik, bind 63, 2017, s. 196–208. Pr. 13. maj 2020: https://www.sciencedirect.com/science/article/pii/S0045790617305347#bib0009

Day, Matt, “Amazon arbejder på en enhed, der kan læse menneskelige følelser,” Bloomberg, 23. maj 2019. Pr. 28. april 2020: https://www.bloomberg.com/news/articles/2019-05-23/amazon-is-working-on-a-wearable-device-that-reads-human-emotions

Forsvarets efterretningstjeneste, “Udfordringer for sikkerhed i rummet”, pressemeddelelse, 11. februar 2019. Pr. 28. april 2020: https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/RUMSIKKERHEDSUDFORDRINGER.PDF

Deichmann, Johannes, Kersten Heineke, Thomas Reinbacher og Dominik Wee, “Creating a Successful Internet of Things Data Marketplace,” McKinsey Digital, oktober 2016. Pr. 3. juli 2019: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/creating-a-successful-internet-of-things-data-marketplace

Derousseau, Ryan, “Teknologien der sporer dine bevægelser på arbejdet,” BBC News, 14. juni 2017. Pr. 28. april 2020: https://www.bbc.com/worklife/article/20170613-the-tech-that-tracks-your-movements-at-work

Dinh-Le, Catherine, Rachel Chuang, Sara Chokshi og Devin Mann, “Bærbar sundhedsteknologi og integration af elektroniske patientjournaler: Omfangsanalyse og fremtidige retninger,” JMIR Mhealth Uhealth, Vol. 7, nr. 9, 2019, s. e12861.

Doffman, Zak, “Ny Pentagon-laser identificerer højrisikoindivider ved hjælp af deres hjerteslag,” Forbes, 27. juni 2019. Pr. 28. april 2020: https://www.forbes.com/sites/zakdoffman/2019/06/27/us-military-laser-can-identify-people-by-their-heartbeats-mit-reports/#6e40b06b2dc6

Dolley, Shawn, “Big datas rolle i præcisionsfolkesundhed,” Frontiers in Public Health, bind 6, 2018, s. 68.

Donahue, Michelle, “Hvordan en farveblind kunstner blev verdens første cyborg,” National Geographic, 3. april 2017. Pr. 28. april 2020: https://news.nationalgeographic.com/2017/04/worlds-first-cyborg-human-evolution-science/

Downey, CL, S. Chapman, R. Randell, JM Brown og D. G. Jayne, “Virkningen af kontinuerlig versus intermitterende overvågning af vitale tegn på hospitaler: En systematisk gennemgang og narrativ syntese,” International Journal of Nursing Studies, bind 84, 2018, s. 19–27.

Edinburgh Law School, MacCormick Fellow Seminar: Prof Andrea Matwyshyn, YouTube-video, 23. oktober 2018. Fra 28. april 2020: https://www.youtube.com/watch?v=7Cs0yc9u-VE

Emondi, Al, “Næste generation af ikke-kirurgisk neuroteknologi,” Forsvarets avancerede forskningsprojektagentur, hjemmeside, udateret. Pr. 28. april 2020: https://www.darpa.mil/program/next-generation-nonsurgical-neurotechnology

Entzeridou, Eleni, Evgenia Markopoulou og Vasiliki Mollaki, “Offentlighedens og lægers forventninger og etiske bekymringer vedrørende elektroniske patientjournaler: Fordelene opvejer risiciene bortset fra informationssikkerhed,” International Journal of Medical Informatics, bind 110, 2018, s. 98–107.

Etherington, Darrell, “Elon Musks Neuralink ser ud til at begynde at udstyre menneskelige hjerner med hurtigere input og output fra næste år,” TechCrunch, 16. juli 2019. Pr. 28. april 2020: https://techcrunch.com/2019/07/16/elon-musks-neuralink-looks-to-begin-outfitting-human-brains-with-faster-input-and-output-starting-next-year/

Faiola, Anthony og Richard J. Holden, “Forbrugernes sundhedsinformatik: Styrkelse af sundhedssøgende gennem mHealth,” Progress in Cardiovascular Diseases, bind 59, nr. 5, 2017, s. 479–486.

Fanucci, Luca, Sergio Saponara, Tony Bacchillone, Massimiliano Donati, Pierluigi Barba, Isabel Sanchez-Tato og Cristina Carmona, “Sensorer og sensorsignalbehandling til fjernovervågning af vitale tegn hos patienter med hjertesvigt,” IEEE Transactions on Instrumentation and Measurement, bind 62, 2013, s. 553–569.

Farivar, Cyrus, “'Stop cyborgerne' lancerer offentlig kampagne mod Google Glass,” Ars Technica, 22. marts 2013. Pr. 9. juli 2019: https://arstechnica.com/tech-policy/2013/03/stop-the-cyborgs-launches-public-campaign-against-google-glass/

FDA—Se den amerikanske fødevare- og lægemiddelstyrelse.

Machine Translated by Google

Federal Trade Commission, "Overholdelse af FTC's regel om anmeldelse af sundhedsbrud", hjemmeside, april 2010. Pr. 28. april, 2020:
https://www.ftc.gov/tips-advice/business-center/guidance/overholdelse af FTCS-regel for underretning om sundhedsbrud

———, "Omhyggelige forbindelser: Opbygning af sikkerhed på internettet" "Things", hjemmeside, januar 2015. Pr. 28. april 2020: https://www.ftc.gov/system/files/documents/plain-language/pdf0199-forsigtigeforbindelser-opbygning af sikkerhedinternetofthings.pdf-fil

FTC—Se den føderale handelskommission.

Garg, Satish K., Stuart A. Weinzimer, William Tamborlane, Bruce A. Buckingham, Bruce W. Bode, Timothy S. Bailey, Ronald L. Brazg, Jacob Illany, Robert H. Slover, Stacey M. Anderson, Richard M. Bergenstal, Benyamin Grosman, Anirban Roy, Toni L. Cordero, John Shin, Scott W. Lee og Francine R. Kaufman, "Glukoseresultater ved hjemmebrug af et hybrid lukket insulinleveringssystem hos unge og voksne med type 1-diabetes," Diabetes Technology & Therapeutics, bind 19, nr. 3, 2017, s. 155–163.

Geller, Stacie E., Abby Koch, Beth F. Pellettiere og Molly Carnes, "Inklusion, analyse og rapportering af køn og race/"Etnicitet i kliniske forsøg: Har vi gjort fremskridt?" Journal of Women's Health, bind 20, nr. 3, 2011, s. 315–320.

Geller, Stacie E., Abigail R. Koch, Pamela Roesch, Amarette Filut, Emily Hallgren og Molly Carnes, "Jo flere ting ændrer sig, jo mere forbliver de de samme: En undersøgelse for at evaluere overholdelse af inklusion og vurdering af kvinder og minoriteter i randomiserede kontrollerede forsøg," Academic Medicine, bind 93, nr. 4, 2018, s. 630–635.

Gillan, Fraser, "Transhumanisterne, der 'opgraderer' deres kroppe," BBC News, 6. oktober 2019. Pr. 11. november 2019: https://www.bbc.com/news/uk-scotland-49893869

Giuliano, Karen, Wan-Ting Su, Daniel Degnan, Kristy Fitzgerald, Richard Zink og Poching DeLaurentis, "Compliance med intravenøs smartpumpe-lægemiddelbibliotek: En beskrivende undersøgelse af 44 hospitaler," Journal of Patient Safety, bind 14, nr. 4, 2018, s. e76–e82.

Glasgow, Russell E., Bethany M. Kwan og Daniel D. Matlock, "Realisering af præcisionssundheds fulde potentiale: Behovet for at inkludere patientrapporteret sundhedsadfærd, mental sundhed, sociale determinanter og patientpræferencer," Journal of Clinical and Translational Science, bind 2, nr. 3, 2018, s. 183–185.

Gonzales, Amy, "Maker digital teknologi sundhedsulighed værre?" Interdisciplinary Association for Population Health Science, 20. november 2017. Pr. 28. april 2020: https://iaphs.org/digital-technology-making-health-inequality-worse/

Goodin, Dan, "Alvorlige fejl gør WPA3 sårbar over for hackere, der stjæler Wi-Fi-adgangskoder," Ars Technica, 11. april 2019. Pr. 28. april 2020: https://arstechnica.com/information-technology/2019/04/alvorlige-fejl-efterlader-wpa3-sårbar-for-hackere-der-stjæler-wi-fi-adgangskoder/

Goodloe, Katharine og Micha Nandaraj Gallo, "Senatet genindfører lov om forbedring af IoT-cybersikkerhed," Inside Privacy, 12. marts 2019. Pr. 3. juli 2019: https://www.insideprivacy.com/internet-of-things/senate-reintroduces-iot-cybersecurity-improvement-act/

Griffin, Patrick, "Rediger dig selv: Biohacking i CRISPR's tidsalder," i Science in the News, 14. februar 2018. Pr. 28. april 2020: http://sitn.hms.harvard.edu/flash/2018/edit-thyself-biohacking-age-crispr/

Groll, Elias, "Det vedvarende mysterium om, hvem der hackede Anthem," Udenrigspolitik, 10. maj 2019. Pr. 28. april 2020: https://foreignpolicy.com/2019/05/10/the-enduring-mystery-of-who-hacked-anthem-hackers-spies-china/

Grush, Loren, "SpaceX kommunikerer med alle undtagen tre ud af 60 Starlink-satellitter en måned efter opsendelsen," The Verge, 28. juni 2019. Pr. 28. april 2020: https://www.theverge.com/2019/6/28/19154142/spacex-starlink-60-satellites-communication-internet-constellation

Gryphon Scientific og Rhodium Group, Kinas bioteknologiske udvikling: Rollen af amerikansk og andet udenlandsk engagement, Washington, DC: US-China Economic and Security Review Commission, 14. februar 2019. Pr. 28. april 2020: https://www.uscc.gov/Research/china%E2%80%99s-biotechnology-development-role-us-and-other-foreign-engagement

Gutierrez, Erie G., Nathan E. Crone, Joon Y. Kang, Yaretson I. Carmenate og Gregory L. Krauss, "Strategier til ikke-EEG-anfaldsdetektion og timing for alarmering og interventioner med tonisk-kloniske anfald," Epilepsia, bind 59, 2018, s. 36-41.

Hambling, David, "Pentagon har en laser, der kan identificere folk på afstand – ved hjælp af deres hjerteslag," MIT Technology Review, 27. juni 2019. Pr. 28. april 2020: https://www.technologyreview.com/s/613891/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/

Harper, Sarah, Ældresamfund: Myter, udfordringer og muligheder, London: Hodder Education, 2006.

Haskins, Caroline, "Afsløret: Dette er Palantirs tophemmelige brugermanual til politiet," Motherboard, 12. juli 2019. Pr. 15. juli, 2019:
https://www.vice.com/en_us/article/9kx4z8/revealed-this-is-palantirs-top-secret-user-manual-for-cops

Healey, Jason, Neal Pollard og Beau Woods, "The Healthcare Internet of Things: Risici og belønninger," Atlantic Council, marts 2015. Pr. 13. juli 2019: https://www.atlanticcouncil.org/images/publications/ACUS_Intel_MedicinskeEnheder.pdf

Koordineringsrådet for sundheds- og folkesundhedssektoren, "Vejledning til cybersikkerhedsarbejdsstyrke inden for sundhedssektoren: Rekruttering og fastholdelse af kvalificerede cybersikkerhedstalenter", udateret. Pr. 30. august 2019: https://healthsectorcouncil.org/wp-content/uploads/2019/06/Vejledning til arbejdsstyrken i sundhedssektoren om cybersikkerhed 1.pdf

Hennessy, Jennifer J., Chanley T. Howell, Michael R. Overly, Jennifer L. Rathburn, Steven M. Millendorf, Aaron K, Tantleff, Samuel D. Goldstick og Thomas E. Chisena, "State Data Breach Notification Laws," hjemmeside, Foley & Lardner LLP, opdateret januar 2019. Pr. 28. april 2020: https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws

Hern, Alex, "Fitness-tracking-appen Strava afslører placeringen af hemmelige amerikanske hærbaser," The Guardian, 28. januar 2018. Pr. 28. april 2020: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Machine Translated by Google

HHS—Se det amerikanske sundhedsministerium.

Holley, Peter, "Bærbar teknologi startet ved at spore skridt". Snart kan det give din chef mulighed for at spore din præstation. Washington Post, 28. juni 2019. Pr. 3. juli 2019: https://www.washingtonpost.com/technology/2019/06/28/bærbar-teknologi-startet-ved-at-spore-skridt-snart-kan-det-give-din-chef-mulighed-for-at-spore-din-performance/?utm_term=.c7692bb4b23a

"Hvordan et produkt opnår ENERGY STAR-mærket", hjemmeside, USA Miljøministeriet, det amerikanske energiministerium, udateret. Pr. 28. april 2020: https://www.energystar.gov/products/how-product-earns-energy-star-label

"Sådan fungerer insulinpumper," webside, Diabetes.co.uk, Diabetes Digital Media, 15. januar 2019. Pr. 28. april 2020: https://www.diabetes.co.uk/insulin/how-insulin-pumps-work.html

Hurley, Dan, "Diabetespatienter hacker sig vej mod en bionisk bugspytkirtel," Wired, 24. december 2014. Pr. 28. april 2020: https://www.wired.com/2014/12/diabetes-patients-hacking-together-diy-bionic-pancreases/

I Am the Cavalry, "Disclosure Programs", hjemmeside, udateret. Pr. 28. april 2020: https://www.iamthecavalry.org/resources/disclosure-programs/

Illinois' generalforsamling, lov om beskyttelse af biometriske oplysninger, 740 Illinois' samlede love 14/1. Pr. 3. juli 2019: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?Akt-ID=3004&Kapitel-ID=57

"Imagining a New Interface: Hands-free Communication Without Saying a Word," webside, Tech@Facebook, 30. juli 2019. Pr. 28. april 2020: https://tech.fb.com/imagining-a-new-interface-hands-free-communication-without-saying-a-word/

International Data Corporation, "Væksten i forbundne IoT-enheder forventes at generere 79,4 ZB data i 2025 ifølge en ny IDC-prognose," 18. juni 2019. Pr. 28. april 2020: https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Jackson, James K., "Komitéen for Udenlandske Investeringer i USA (CFIUS)," Congressional Research Service, RL33388, 23. oktober 2019. Pr. 28. april 2020: https://crsreports.congress.gov/product/pdf/RL/RL33388

Jamoon, Eric, Vaishali Patel, Jennifer King og Michael Furukawa, "Nationale opfattelser af indførelsen af elektroniske patientjournaler: Barrierer, virkninger og føderale politikker," National Conference on Health Statistics 2012, Washington, DC, 6.-8. august 2012.

Jaramillo, Estrella, "Mød de virksomheder inden for kvinders sundhed, der forstyrrer wearable-området," Forbes, 16. maj 2019. Pr. 28. april 2020: https://www.forbes.com/sites/estrellajaramillo/2019/05/16/kvinders-sundhedsvirksomheder-forstyrrer-den-bærbare-plads/#4d36fdb228b3

Kastrenakes, Jacob, "Wi-Fi 6: Er det virkelig så meget hurtigere?" The Verge, 21. februar 2019. Pr. 28. april 2020: https://www.theverge.com/2019/2/21/18232026/wi-fi-6-speed-explained-router-wifi-how-does-work

Khan, Sieeka, "Elektroniske tatoveringer kan laves med grafen og silke," Science Times, 13. marts 2019. Pr. 28. april 2020: https://www.sciencetimes.com/articles/18598/20190313/elektroniske-tatoveringer-lavet-med-grafen-silke.htm

Klitzman, Robert, Er jeg mine gener?: Konfrontation med skæbne og familiehemmeligheder i genetisk testnings tidsalder, Oxford, UK: Oxford University Press, 2012.

Knack, Anna, Advait Deshpande, Stijn Hoorens og Salil Gunashekar, "Wearable Devices: Impplications of Game-Changing Technologies in the Services Sector in Europe," Eurofound, 2019. Pr. 28. april 2020: https://www.rand.org/pubs/external_publications/EP67914.html

Kumar, Shefaili, J. Tran Tran, Wei-Nchih Lee, Ben Bradshaw, Luca Foschini og Jessie Juusola, "Longitudinelle data fra aktivitetsmålere viser, at personer med større uoverensstemmelse i aktivitetsniveauer er mere tilbøjelige til at udvikle mere alvorlig depression," Value in Health, bind 21, 2018, s. S191.

Lai, AM, PYS Hsueh, YK Choi og RR Austin, "Nuværende og fremtidige tendenser inden for forbrugersundhedsinformatik og patient-genererede sundhedsdata," Årbog for medicinsk informatik, bind 26, nr. 01, 2017, s. 152–159.

Larson, Erik, "Kinesisk statsborger tiltalt i forbindelse med Anthem-hack af 80 millioner mennesker," Bloomberg News, 9. maj 2019. Pr. 28. april 2020: https://www.bloomberg.com/news/articles/2019-05-09/chinese-national-indicted-by-us-grand-jury-over-anthem-hack

Lee, Mary, "'Kroppenes internet' skaber farlige præcedenser," Washington Post, 15. oktober 2018. Pr. 13. juli, 2019: https://www.washingtonpost.com/news/theworldpost/wp/2018/10/15/sundhedsdata/?utm_term=.ff1d3a1de516

LeMoyne, Robert, Timothy Mastroianni, Donald Whiting og Nestor Tomycz, Bærbare og trådløse systemer med internetforbindelse til kvantificering af Parkinsons sygdom og essentielle tremorkarakteristika, bind 31, Bærbare og trådløse systemer til sundhedsvæsenet II, Singapore: Springer, 2019.

Leveson, Nancy G., Safeware: Systemsikkerhed og computere, Boston, Massachusetts: Addison-Wesley, 1995.

Lilley, Kevin, "20.000 soldater udtaget til hærens fitnessprograms 2. forsøg," Army Times, 27. juli 2015. Pr. 28. april 2020: https://www.armytimes.com/news/your-army/2015/07/27/20000-soldater-ansat-til-hærens-fitnessprogram-2.-prøve/

Linder, Courtney, "Hvorfor denne softwareingeniør implanterede en Tesla-parkeringsnøgle i sin arm," Popular Mechanics, 14. august 2019. Pr. 28. april 2020: https://www.popularmechanics.com/technology/infrastructure/a28698503/tesla-nøgleimplantat/

Lupton, Deborah, "Kvantificering af kroppen: Overvågning og måling af sundhed i M-sundhedsteknologiernes tidsalder," Critical Public Health, bind 23, nr. 4, 2013, s. 393–403.

———, "Kritiske perspektiver på digitale sundhedsteknologier" Sociologikompas, bind 8, nr. 12, 2014, s. 1344–1359.

MacMillan, Douglas, "Datamæglere sælger dine hemmeligheder". "Hvordan stater forsøger at stoppe dem," Washington Post, 24. juni 2019. Pr. 3. juli 2019: https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/?utm_term=.a46f70fcae28

Machine Translated by Google

Manadhata, Pratyusa K., og Jeannette M. Wing, “En angrebsoverflademetrik,” IEEE Transactions on Software Engineering, bind 37, nr. 3, 2010, s. 371–386.

Marmot, Michael, “Sociale determinanter for sundhedsuligheder,” The Lancet, bind 365, nr. 9464, 2005, s. 1099–1104.

Marr, Bernard, “Hvor meget data skaber vi hver dag? De sindssyge statistikker, som alle burde læse,” Forbes, 21. maj 2018. Pr. 30. august 2019: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2df2278360ba

———, “Kunstig intelligens i dit toilet. Ja, virkelig!” Forbes, 20. maj 2019a. Pr. 28. april 2020: https://www.forbes.com/sites/bernardmarr/2019/05/20/kunstigt-intelligente-toiletter-ja-de-er-her/2/#477336615a85

———, “Kinesisk social kreditvurdering: Utopisk big data-lykke eller sort spejl på steroider?” Forbes, 21. januar 2019b. Pr. 28. april 2020: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/

Massachusetts Institute of Technology Media Lab, “Projekt AttentivU”, pressemeddelelse, 20. august 2019. Pr. 30. august 2019: https://www.media.mit.edu/projects/attentivu/overview/

Matwyshyn, Andrea M., “Bodies internet”, 9. årlige konference for lærde inden for privatlivsret, Berkeley Center for Law & Technology, Washington, DC, 2. juni 2016. Pr. 28. april 2020: https://www.law.berkeley.edu/research/bclt/past-events/2016-konferencer/juni-2016-den-9.-årlige-konference-for-privatlivsretsforskere/program/

———, "'Kroppenes internet' er her. Er domstole og "Er tilsynsmyndighederne klar?" Wall Street Journal, 12. november 2018. Pr. 28. april 2020: https://www.wsj.com/articles/the-internet-of-bodies-is-here-are-courts-and-regulators-ready-1542039566

———, “Kroppenes internet,” William & Mary Law Review, bind 77, nr. 1, 2019. Pr. 28. april 2020: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3452891

MDIC—Se Konsortium for innovation af medicinsk udstyr.

Medical Device Innovation Consortium, Rapport om cybersikkerhed inden for medicinsk udstyr: Fremme af koordineret offentliggørelse af sårbarheder, Minneapolis, Minn., 1. oktober 2018. Pr. 3. juli, 2019: http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf

Meingast, Marci, Tanya Roosta og Shankar Sastry, “Sikkerheds- og privatlivsproblemer med informationsteknologi inden for sundhedsvæsenet,” Proceedings of the 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, New York, 31. august–3. september 2006, s. 5453–5458.

Morris, David, “Træningsapp når FTC-forlig på 1 million dollars efter at have brudt sit løfte om at betale brugere for træning,” Fortune, 23. september 2017. Pr. 28. april 2020: https://fortune.com/2017/09/23/exercise-app-pact-settlement/

Moss, Sebastian, “USA sanktionerer kinesiske tech-virksomheder, herunder Sensetime, for krænkelser af menneskerettighederne,” Data Center Dynamics, 8. oktober 2019. Pr. 28. april 2020: https://www.datacenterdynamics.com/news/us-sanctions-chinese-tech-companies-including-sensetime-over-human-rights-abuses/

Mulligan, Stephen P., Wilson C. Freeman og Chris D. Linebaugh, Databeskyttelseslovgivning: En oversigt, Washington, DC: Congressional Research Service, R45631, 25. marts 2019. Pr. 28. april 2020: https://crsreports.congress.gov/product/pdf/R/R45631

National Association of Attorneys General, “Høringer i den føderale handelskommission om konkurrence og forbrugerbeskyttelse Beskyttelse i det 21. århundrede: Offentlige kommentarer fra 43 statsadvokater,” 11. juni 2019. Pr. 20. april 2020: https://www.washingtonpost.com/context/state-ags-call-for-data-regulations/52f85d7a-c512-4eec-bc50-2ac411e2c593/

National Center for Health Statistics, “Sundhed, USA, 2015: Med særligt fokus på racemæssig og etnisk sundhed "Uligheder," 2016.

National Institute of Standards and Technology, “NIST-udgivelser "Udkast til anbefalinger til sikkerhedsfunktioner for IoT-enheder", pressemeddelelse, 1. august 2019. Pr. 7. juli 2020: https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices

Nationalt Institut for Standarder og Teknologi Cyberfysisk Offentlig Systemarbejdsgruppe, “Rammeværk for cyber-fysisk Systems, version 1.0,” maj 2016. Pr. 28. april 2020: https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Rammeværk_for_Cyberfysiske_Systemer_Udgivelse_1_0Endelig.pdf

Neal, Meghan, “Internet of Bodies Is Coming, and You Could Get Hacked” (Kroppenes internet kommer, og du kan blive hacket), Motherboard, 13. marts 2014. Pr. 3. juli, 2019: https://www.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked

Forskning og udvikling inden for netværk og informationsteknologi, “Cyber-Physical System Interagency Working Group (2015) CPS Vision Statement,” 3. juni 2015. Pr. 7. november 2019: https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Visionserklæring_Fysiske_Systemer_(CPS).pdf

Newhouse, William, Stephanie Keith, Benjamin Scribner og Greg Witte, “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,” NIST Special Publication 800-181, august 2017. Pr. 28. april 2020: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Ng, Alfred, “Sikkerhedsfejl muliggør spionage over 5G, advarer forskere,” CNET, 1. februar 2019. Pr. 28. april 2020: https://www.cnet.com/news/security-flaw-allows-for-spying-over-5g-researchers-find/

NIST—Se National Institute of Standards and Technology.

NITRD—Se Netværks- og informationsteknologiforskning og Udvikling.

Oberhaus, Daniel, “Dette gør-det-selv-implantat giver dig mulighed for at streame film” "fra indersiden af dit ben," Wired, 30. august 2019. Pr. 30. august 2019: https://www.wired.com/story/this-diy-implant-lets-you-stream-movies-from-inside-your-leg/

Kontoret for den nationale koordinator for sundhedsinformation Teknologi, websiden “Hvad er en elektronisk patientjournal (EHR)?”, HealthIT.gov, 10. september 2019. Pr. 28. april 2020: https://www.healthit.gov/faq/what-electronic-health-record-ehr

Machine Translated by Google

"Officielle tidslinjer for IEEE 802.11-arbejdsgruppens projekter"
Institut for Elektronik- og Elektronikingeniører, 25. september 2019. Pr. 28.
april 2020: http://www.ieee802.org/
11/Reports/802.11_Timelines.htm

Okun, Michael S., "Tips til valg af en enhed til dyb hjernestimulering," JAMA
Neurology, bind 76, nr. 7, april 2019, s. 749–750.

Osoba, Osonde A., og William Welser IV, En intelligens i vores billede:
Risikoen for bias og fejl i kunstig intelligens, Santa Monica, Californien: RAND
Corporation, RR-1744-RC, 2017. Pr. 28. april 2020: https://www.rand.org/pubs/
research_reports/
RR1744.html

Papola, Davide, Chiara Gastaldon og Giovanni Ostuzzi, "Kan et digitalt
medicinsystem forbedre overholdelse af antipsykotisk behandling?"
Epidemiology and Psychiatric Sciences, bind 27, nr. 3, 2018, s. 227–
229.

Piwek, Lukasz, David A. Ellis, Sally Andrews og Adam Joinson,
"Fremkomsten af forbrugersundhedswearables: Løfter og barrierer," PLoS
Medicine, bind 13, nr. 2, 2016, s. e1001953.

Plowman, R. Scooter, Timothy Peters-Strickland og George M. Savage,
"Digitale lægemidler: Klinisk gennemgang af sikkerheden af tabletter med
sensorer," Ekspertudtalelse om lægemiddelsikkerhed, bind 17, nr. 9, 2018,
s. 849–852.

Purcell, David, H. Irene Hall, Kyle L. Bernstein, Thomas L. Gift, Eugene
McCray og Jonathan Mermin, "Betydningen af populationsnævnere for
stor folkesundhed for marginaliserede befolkningsgrupper," JMIR Public
Health and Surveillance, bind 2, nr. 1, 17. maj 2016, s. e26.

Ratnam, Gopal, "Fremskridt med den føderale lov om databeskyttelse går langsommere
i begge kamre," Chicago Tribune, 26. juni 2019. Pr. 8. juli 2019: https://

www.chicagotribune.com/sns-tns-bc-congress-data-privacy-20190626-story.html

Revideret Washington-lov, kapitel 19.375, Biometriske identifikatorer.
Fra 3. juli 2019: https://
app.leg.wa.gov/RCW/default.aspx?cite=19.375

Ross, Julianne, "Smarte vægte måler meget mere end vægt,"
CNN, 4. januar 2019. Pr. 28. april 2020: https://
www.cnn.com/2019/01/04/cnn-underscored/best-smart-scales/index.html

Rupert, Douglas J., Rebecca R. Moultrie, Jennifer Gard Read, Jacqueline
B. Amoogegar, Alexandra S. Bornkessel, Amie C.
O'Donoghue og Helen W. Sullivan, "Opfattede reaktioner fra
sundhedsudbydere på patienters og pårørendes brug af online
sundhedsfællesskaber," Patient Education and Counseling, bind 96,
nr. 3, 2014, s. 320–326.

Russo, Massimo og Michael Albert, "Sådan vil IoT-dataøkosystemer
transformere B2B-konkurrencen," Boston Consulting Group, 27. juli 2018.
Pr. 3. juli 2019: https://www.bcg.com/
en-us/publications/2018/how-internet-of-things-iot-data-ecosystems-transform-
b2b-competition.aspx

Samuel, Sigal, "Hvordan biohackere forsøger at opgradere deres hjerner,
deres kroppe – og menneskets natur," *Vox,* 25. juni 2019.
Pr. 28. april 2020: https://
www.vox.com/future-perfect/2019/6/25/18682583/
biohacking-transhumanisme-menneskelig-augmentation-genteknologi-
crispr

Savage, Maddy, "Tusindvis af svenskere indsætter mikrochips under huden,"
NPR, 22. oktober 2018. Pr. 28. april 2020: https://www.npr.org/
2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-
under-their-skin

Schneeweiss, Sebastian og Jerry Avorn, "En gennemgang af anvendelsen
af sundhedsdatabaser til epidemiologisk forskning i behandlinger," Journal
of Clinical Epidemiology, bind 58, nr. 4, 2005, s. 323–337.

Schulte, Fred og Erika Fry, "Død med 1.000 klik: Hvor elektroniske
patientjournaler gik galt," Kaiser Health News, 18. marts 2019a. Pr. 28.
april 2020: https://khn.org/news/death-by-a-
thousand-clicks/

———, "FDA-chef opfordrer til strengere kontrol af elektroniske
patientjournaler," Kaiser Health News, 21. marts 2019b. Pr. 28. april 2020:
https://khn.org/
news/fda-chief-calls-for-stricter-scrutiny-of-electronic-health-records/

Scott, Emily, "Wearable Device Can Predict Older Adults' Risk of
Falling" (Bærbar enhed kan forudsige ældre voksnes risiko for at falde),
Carl R. Woese Institute For Genomic Biology, University of Illinois,
12. juli 2018. Pr. 28. april 2020: https://www.igb.illinois.edu/article/wearable-
device-can-predict-older-adults-risk-falling

"Security Breach Notification Laws," database, National Conference
of State Legislatures, Washington, DC, opdateret 29. september 2018.
Pr. 28. april 2020: http://www.ncsl.org/research/
telecommunications-and-information-technology/security-breach-
notification-laws.aspx

Silver, Mike, "Forskere udvikler små tandmonterede sensorer, der kan
spore, hvad du spiser," Tufts Now, 22. marts 2018. Pr. 9. juli 2019: https://
now.tufts.edu/
news-releases/scientists-develop-tiny-tooth-mounted-sensors-can-track-
what-you-eat

Simons, Joseph, Kontoret for formanden, Federal Trade
Commission, "Joseph Simons til den ærede Frank Pallone, Jr., Washington,
DC," brev, 1. april 2019. Pr. 28. april 2020: https://energycommerce.house.gov/
sites/democrats.
energycommerce.house.gov/files/documents/FTC%20
Svar%20til%20Pallone-Schakowsky.pdf

Slager, Heidi K., Jamie Jensen, Kristin Kozlowski, Holly Teagle,
Lisa R. Park, Allison Bieve og Megan Mears, "Fjernprogrammering af
cochleaimplantater," Otology & Neurotology, bind 40, nr. 3, 2019, s. e260.

Smith, Robert Ellis, "Samling af statslige og føderale privatlivslove 2013
elektronisk udgave", webside, Privacy Journal, 2013.

Solon, Olivia, "Amazon patenterer armbånd, der sporer
lagerarbejderes bevægelser," The Guardian, 13. januar 2018. Pr. 28. april
2020: https://www.theguardian.com/
technology/2018/jan/31/amazon-warehouse-wristband-tracking

Stachel, Joshua R., Ervin Sejdiÿ, Ajay Ogirala og Marlin Mickle,
"Virkningen af tingenes internet på implanterede medicinske apparater,
herunder pacemakere og ICD'er," 2013 IEEE International Instrumentation
and Measurement Technology Conference (I2MTC), Minneapolis, Minn.,
6.-9. maj 2013. Pr. 28. april 2020: https://ieeexplore.ieee.org/document/
6555533

Staedter, Tracy, "Satellitinternetteknologi har antændt et nyt rumkapløb," Now.,
Northrup Grumman, 3. juli 2019. Pr. 28. april 2020: https://

now.northropgrumman.com/satellite-internet-technology-has-
ignited-a-new-space-race

Steele, Robert og Andrew Clarke, "Tingenes internet og næste
generations informationssystemer for folkesundhed",
Kommunikation og netværk, bind 5, nr. 03, 2013, s. 4–9.

Machine Translated by Google

Strathspey Crown, “Strathspey Crown LLC annoncerer udstedelse af amerikansk patent for den første implanterbare intraokulære linse (IOL) med videokamera og trådløs transmissionsfunktion,” 12. juli 2017. Pr. 28. april 2020: http://strathspeycrown.com/assets/

pdf/1505148854250fc4abc8da4e88d59bf6d0486bf1cc.pdf

Stück, David, Haraldur Tómas, Greg Ver Steeg, Alessandro Epasto og Luca Foschini, “Nye digitale stemmebiomarkører for demens fra Framingham-studiet,” Alzheimer's & Dementia: The Journal of the Alzheimer's Association, bind 14, nr. 7, 2018, s. 778–779.

Sullivan, Tom, “Hvorfor EHR-datainteroperabilitet er sådan et rod i 3 diagrammer,” Healthcare IT News, 16. maj 2018. Pr. 28. april 2020: https://www.healthcareitnews.com/news/

why-ehr-data-interoperability-such-mess-3-charts

Swearingen, Jake, “Europas 'ret til at blive glemt' vil blive i Europa,” New York Magazine, 10. januar 2019. Pr. 28. april 2020: http://nymag.com/intelligencer/2019/01/europes-right-to-be-forgotten-will-be-staying-in-europe.html

Texas' erhvervs- og handelslov, afsnit 11, underafsnit A, kapitel 503, biometriske identifikatorer. Pr. 28. april 2020: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

“Argumentet mod retten til at blive glemt,” Law Times, 17. september 2018. Pr. 28. april 2020: https://www.lawtimesnews.com/article/the-case-against-a-right-to-be-forgotten-16216/

Kroppernes internet, “Chat angående IoB–FTC-kommunikation @ "TerrellMcSweeny & @amatwyshyn," Twitter-øjeblik, 7. marts 2018. Pr. 28. april 2020: https://twitter.com/i/moments/1062106824449634304

ThreatConnect Research Team, “The Anthem Hack: All Roads Lead to China,” ThreatConnect blog, 27. februar 2015. Pr. 28. april 2020: https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/

Tibken, Shara og Robert Cheng, “Høreapparater bliver smartere. Tænk på AI og sundhedsovervågning,” CNET, 5. april 2018. Pr. 9. juli 2019: https://www.cnet.com/news/hearing-aids-now-theyre-internet-ai-and-health-devices-starkey-oticon-harman-bose/

Trammell, Dustin D., “Forskelle: Bodyhacking vs. Biohacking,” i BodyHackingCon-bloggen, 26. september 2015. Pr. 28. april, 2020:

https://bodyhackingcon.com/blog/differences-bodyhacking-vs-biohacking.html

Trauth, Erin og Ella Browning, “Teknologiseret tale: Bærbare teknologier, patienthandlekraft og medicinsk kommunikation i sundhedsvæsenet,” International Journal of Sociotechnology and Knowledge Development (IJSKD), bind 10, nr. 3, 2018, s. 1–26.

Turk, Victoria, “Denne søvnsporingsring kan opdage, når du har drukket for meget,” Wired, 18. juni 2019. Pr. 28. april, 2020:

https://www.wired.co.uk/article/oura-ring-uk-sleep-tracking

FN, Verdensbefolkningens aldring 2015 (ST/ESA/SER.A/390), New York: FN's Departement for Økonomiske og Sociale Anliggender, Befolkningsafdeling, 2015.

University of Southern California Center for Body Computing, “Cybersikkerhed i sundhedsvæsenet: Hvordan californisk erhvervsliv kan føre an”, hvidbog, 2018. Pr. 28. april 2020: https://www.uscbodycomputing.org/uncensored/2018/9/24/z6l7c4u7dmu6dqi1e5rvmc7hhujlh6

US Code, Titel 15, Paragraf 45, Urimelige konkurrencemetoder Ulovlige; Forebyggelse foretaget af Kommissionen.

Den amerikanske forbrugerproduktsikkerhedskommission, “Provata Health tilbagekalder aktivitetsmålere til salgsfremmende formål på grund af fare for forbrændinger,” 25. september 2018. Pr. 27. april 2020: https://www.cpsc.gov/Recalls/2018/Provata-Health-Recalls-Promotional-Activity-Trackers-Due-to-Burn-Hazard

Det amerikanske sundhedsministerium, “Afdødes helbredsoplysninger: 45 CFR 160.103, paragraf (2)(iv) i definitionen af 'beskyttede helbredsoplysninger'”

September 2013. Pr. 28. april 2020: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/helbredsoplysninger-for-afdøde-personer/indeks.html

Den amerikanske fødevare- og lægemiddelstyrelse (FDA), “Vejledning til industrien: Cybersikkerhed for netværksforbundne medicinske apparater, der indeholder standardsoftware (OTS), 14. januar 2005. Pr. 3. juli 2019: https://www.fda.gov/media/72154/download

———, “Håndtering af cybersikkerhed i medicinsk udstyr efter markedsføring: Vejledning til personale i industrien og fødevare- og lægemiddelstyrelsen,” 28. december 2016. Pr. 28. april 2020: https://www.fda.gov/media/95862/download

———, "Indhold af præmarkedsindsendelser til håndtering af Cybersikkerhed i medicinsk udstyr: Udkast til vejledning til personale i industrien og fødevare- og lægemiddelstyrelsen," 18. oktober 2018. Pr. 3. juli 2019: https://www.fda.gov/media/86174/download

———, "FDA godkender første kontinuerlige glukosemåling" "System med en fuldt implanterbar glukosesensor og kompatibel mobilapp til voksne med diabetes," pressemeddelelse, 25. juni 2018b. Pr. 28. april 2020: https://www.fda.gov/news-events/press-announcements/fda-approves-first-continuous-glucose-monitoring-system-fully-implantable-glucose-sensor-and

———, “Oversigt over medicinsk udstyr”, webside, 14. september 2018a. Pr. 28. april 2020: https://www.fda.gov/industry/regulated-products/medical-device-overview

———, "Tilbagekaldelser af medicinsk udstyr", hjemmeside, 26. september 2018c. Pr. 28. april 2020: https://www.fda.gov/medical-devices/medical-device-safety/tilbagekaldelser af medicinsk udstyr

———, “Cybersikkerhed”, webside, 27. juni 2019a. Pr. 3. juli, 2019:

https://www.fda.gov/medical-devices/digital-health/cybersikkerhed

———, “Cybersikkerhedssårbarheder, der påvirker Medtronics implanterbare hjerteenheder, programmeringsenheder og hjemmemonitorer: FDA's sikkerhedsmeddelelse,” webside, 21. marts 2019b. Pr. 28. april 2020: https://www.fda.gov/medical-devices/safety-communications/cybersikkerhedssårbarheder, der påvirker Medtronic implanterbare hjerteenheder, programmører og hjemmet

Machine Translated by Google

———, “Offentlig workshop—Indhold af præmarkedsindsendelser til håndtering af cybersikkerhed i medicinsk udstyr 29.-30. januar 2019,” webside, januar 2019c. Pr. 28. april 2020: https://www.fda.gov/medical-devices/workshops-conferences-medical-devices/public-workshop-content-premarket-submissions-management-cybersecurity-medical-devices-january-29-30

US Immigration and Customs Enforcement (ICE), “Initiativ til deling af information om retshåndhævelse”, hjemmeside, USA Ministeriet for Indenrigssikkerhed, udateret. Pr. 28. april 2020:
https://www.ice.gov/le-information-sharing

Vaas, Lisa, “Læger deaktiverede trådløs teknologi i Dick Cheneys pacemaker for at forhindre hacking,” Naked Security, 22. oktober 2013. Pr. 28. april 2020: https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/

Verheij, Robert A., Vasa Curcin, Brendan C. Delaney og Mark M. McGilchrist, “Mulige kilder til bias i brugen og genbrugen af elektroniske patientjournaldata i primær sundhedsvæsen,” Journal of Medical Internet Research, bind 20, nr. 5, 2018, s. e185.

Vermont Public Law H.764 (lov 171), en lov vedrørende datamæglere og forbrugerbeskyttelse, 22. maj 2018. Pr. 28. april 2020: https://legislature.vermont.gov/bill/
status/2018/H.764

Vita-More, Natasha, “Life Extension Leadership Meetings, Conferences, and Festivals,” H Plus Magazine, 22. juli 2018.

Wang, Echo, “Kinas Kunlun-teknologiselskab accepterer amerikansk krav om at sælge Grindr-datingappen til homoseksuelle,” Reuters, 13. maj 2019. Pr. 28.
april 2020: https://www.reuters.com/article/us-grindr-ma-beijingkunlun/chinas-kunlun-tech-accepterer-os-efterspørgsel-om-at-sælge-grindr-gay-dating-app-idUSKCN1SJ28N

Waters, Michael, “Den smarte ble kommer. Hvem vil egentlig have den?” Vox, 2. maj 2019. Pr. 28. april 2020: https://www.vox.com/the-goods/2019/5/2/18525487/smart-diaper-huggies-monit-pampers-alert-poop-pee

Wee, Sui-Lee, “Kina bruger DNA til at spore sin befolkning med hjælp fra amerikansk ekspertise,” New York Times, 21. februar 2019. Pr. 3. juli 2019: https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html

Whittaker, Zack, “Justitsministeriet anklager kinesisk hacker for brud på Anthem-sikkerhedsdokumentet i 2015,” TechCrunch, 9. maj 2019. Pr. 28. april 2020:
https://techcrunch.com/2019/05/09/anthem-breach-indictment

Wicklund, Eric, “FDA godkender mHealth-wearable til sporing af epileptiske anfald,” mHealth Intelligence, 6. februar 2018. Pr. 29. april 2020: https://mhealthintelligence.com/news/fda-approves-mhealth-wearable-for-tracking-epileptic-seizures

Wisconsin-lovgivningen §134.98, Meddelelse om uautoriseret erhvervelse af personlige oplysninger. Pr. 29. april 2020: https://docs.legis.wisconsin.gov/statutes/statutes/134/98

Woods, Beau, Andrea Coravos og Joshua David Corman, “Argumenter for en hippokratisk ed for forbundne medicinske apparater: Synspunkt,” *Journal of Medical Internet Research,* bind 21, nr. 3, 2019. Pr. 3. juli 2019: https://www.jmir.org/2019/3/e12568/pdf

Wootson, Cleve R., “En mand beskrev sin flugt fra et brændende hus. Hans pacemaker fortalte politiet en anden historie,” *Washington Post,* 8. februar 2017. Pr. 3. juli 2019: https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-sin-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/?utm_term=.f0b9a4d2b9dd

Verdenssundhedsorganisationen, "Ikke-smitsomme sygdomme", faktablad, 1. juni 2018. Pr. 28. april 2020: https://www.who.int/news-room/fact-sheets/detail/ikke-smitsomme sygdomme

Yang, Tingting, Dan Xie, Zhihong Li og Hongwei Zhu, “Nylige fremskridt inden for bærbare taktile sensorer: Materialer, følemekanismer og enhedsydelse,” *Materials Science and Engineering: R: Reports,* bind 115, 2017, s. 1–37.

Yu, Kun-Hsing og Isaac S. Kohane, “Indramning af udfordringerne ved kunstig intelligens i medicin,” *BMJ Quality & Safety,* Bind 28, 2019, s. 238–241.

Zaino, Jennifer, “5G vs. 4G mobilteknologi: Hvad virksomheder har brug for at vide,” *BizTech,* 6. august 2019. Pr. 29. april 2020: https://biztechmagazine.com/article/2019/09/5g-vs-4g-cellular-technology-what-businesses-need-know-perfcon

Zhang, Sarah, “Folk råber op om at købe gamle insulinpumper,” *The Atlantic,* 29. april 2019. Pr. 7. juli 2020: https://www.theatlantic.com/science/archive/2019/04/looping-created-insulin-pump-underground-market/588091/

Zlotolow, Dan A., og Scott H. Kozin, “Fremskridt inden for proteser til øvre ekstremiteter,” *Hand Clinics,* bind 28, nr. 4, 2012, s. 587–593.

Zraick, Karen og Sarah Mervosh, “Den søvntracker kunne forværre din søvnløshed,” *New York Times,* 13. juni 2019. Pr. 29. april 2020: https://www.nytimes.com/2019/06/13/health/sleep-tracker-insomnia-orthosomnia.html?module=inline

Machine Translated by Google

Taksigelser

Forfatterne er dybt taknemmelige for Jacques Dubois' generøse donation til RANDs Center for Global Risk and Security (CGRS), som gjorde dette arbejde muligt. Forfatterne takker også CGRS' rådgivende bestyrelse samt Robin Meili, King Mallory og Casey Bouskill for at have gjort dette projekt muligt.

Vi vil gerne takke Caolionn O'Connell for rådgiver for teamet og Sonni Efron for hendes dygtige redaktionelle assistance. Vi vil også gerne takke vores korrekturlæsere, Marjory Blumenthal, senior policyforsker ved RAND Corporation, og Patricia Stapleton, forsker i komparativ statskundskab og offentlig politik ved RAND, for deres tankevækkende kommentarer til denne rapport, og Rick Penn-Kraus for hans illustrationer.

Vi vil også gerne takke følgende personer for værdifulde diskussioner og indsigter: Penny Chase, James Christensen, Steven Christey, Al Emondi, Angel Giuffria, Amal Graafstra, Matthew Hepburn, Timothy Hanson, Robert Klitzman og Beau Woods.

Eventuelle fejl i denne artikel er forfatternes egne.

Om forfatterne

Mary Lee er matematiker ved RAND Corporation og indledende fellow for RANDs Center for Global Risk and Security. Hendes forskningsinteresser omfatter matematisk modellering og simulering af komplekse systemer inden for forsvar/
rumfart, cyberpolitik samt sundhedspleje og kroniske sygdomme.

Benjamin Boudreaux er professor ved Pardee RAND Graduate School og policyforsker ved RAND, der arbejder i krydsfeltet mellem national sikkerhed, teknologi og etik. Hans nuværende forskning fokuserer på etiske spørgsmål inden for kunstig intelligens, social mediepolitik og cyberhændelser.

Ritika Chaturvedi var ingeniør hos RAND Corporation under dette projekt. Hun arbejder i øjeblikket som forsker ved Schaeffer Center for Health Policy and Economics ved University of Southern California. Hun har en bred baggrund inden for ingeniørvidenskab, videnskabs- og teknologipolitik, aktivvurdering, strategisk rådgivning og translationel biomedicinsk forskning. Hun er interesseret i videnskabelige og teknologiske spørgsmål vedrørende de brede virkninger af nye, disruptive teknologier inden for biovidenskab og sundhedspleje samt på samfundet.

Sasha Romanosky er policyforsker hos RAND Corporation og tidligere cyberpolitisk rådgiver for Pentagon i forsvarsministerens kontor for politik. Han forsker i emner inden for sikkerheds- og privatlivsøkonomi, national sikkerhed, anvendt mikroøkonomi samt jura og økonomi.

Bryce Downing er forskningsassistent hos RAND Corporation. Før han kom til RAND, var han praktikant i strategiske simuleringer på US Army War College, Center for Strategic Leadership. Hans forskningsinteresser omfatter teknologipolitik, modellering af beslutningstagning under usikkerhed og national sikkerhed.

Machine Translated by Google

Om denne rapport

Det arbejde, der er beskrevet i denne rapport, blev udført som en del af et stipendium tildelt af RAND Corporations Center for Global Risk and Security. Denne rapport beskriver nye teknologier, heri benævnt Internet of Bodies; analyserer deres fordele og risici; og foreslår måder, hvorpå forskellige interessenter kan afbalancere disse fordele og risici. Denne rapport bør være af interesse for den brede offentlighed, Internet of Bodies og producenter af medicinsk udstyr, sundhedspersonale og politiske beslutningstagere. Forskningen blev udført i Center for Global Risk and Security mellem februar 2019 og september 2019.

Finansiering

Finansieringen af denne rapport blev leveret af en generøs bevilling fra Jacques Dubois.

Om RAND Center for Global Risiko og Sikkerhed

Center for Global Risk and Security arbejder på tværs af RAND Corporation for at udvikle tværfaglig forskning og politisk analyse, der beskæftiger sig med systemiske risici for global sikkerhed. Centret trækker på RANDs ekspertise til at supplere og udvide RAND-forskning på mange områder, herunder sikkerhed, økonomi, sundhed og teknologi. Et udvalg af fremtrædende erhvervsledere, filantroper og tidligere politikere rådgiver og støtter centrets aktiviteter, som i stigende grad fokuserer på globale sikkerhedstendenser og virkningen af disruptive teknologier på risiko og sikkerhed. For mere information om RAND Center for Global Risk and Security, besøg www.rand.org/international/

cgrs.

RAND Corporation er en forskningsorganisation, der udvikler løsninger på offentlige politiske udfordringer for at hjælpe med at forbedre lokalsamfund overalt
verden mere sikker og tryg,
sundere og mere velstående.
RAND er nonprofitorganisation, upartisk og engageret i offentlighedens interesse.

RANDs publikationer afspejler ikke nødvendigvis meningerne hos dets forskningsklienter og sponsorer. er et RAND® registreret varemærke.

Begrænset trykt og elektronisk Distributionsrettigheder

Dette dokument og varemærket/ varemærkerne heri er beskyttet af loven. Denne repræsentation af RANDs intellektuelle ejendom er kun til ikke-kommerciel brug. Uautoriseret offentliggørelse af denne publikation online er forbudt.
Der gives tilladelse til at kopiere dette dokument kun til personlig brug, så længe det er uændret og fuldstændigt.
Der kræves tilladelse fra RAND til at reproducere eller genbruge vores forskningsdokumenter i en anden form til kommerciel brug. For information
For tilladelser til genoptryk og linkning, besøg venligst www.rand.org/pubs/ tilladelser.

For mere information om dette publikation,
besøg www.rand.org/t/RR3226.

© 2020 RAND Corporation

Machine Translated by Google

Internetforbundne "smarte" enheder bliver i stigende grad tilgængelige på markedet, hvilket lover forbrugere og virksomheder forbedret bekvemmelighed og effektivitet. Inden for dette bredere Internet of Things (IoT) ligger en voksende industri af enheder, der overvåger menneskekroppen og overfører de indsamlede data via internettet. Denne udvikling, som nogle har kaldt Internet of Bodies (IoB), inkluderer en voksende

en række enheder, der kombinerer software, hardware og kommunikationsfunktioner til at spore personlige sundhedsdata, yde vital medicinsk behandling eller forbedre kropslig komfort, funktion, sundhed eller velvære.

Disse enheder komplicerer dog også et felt, der allerede er fyldt med juridiske, lovgivningsmæssige og etiske risici. Forfatterne af denne rapport undersøger denne nye samling af menneskekropscentrerede og internetforbundne teknologier; udforsker fordele, sikkerheds- og privatlivsrisici samt etiske implikationer; undersøger det spirende lovgivningslandskab for disse enheder og de data, de indsamler; og fremsætter anbefalinger til

balancere IoB-risici og -belønninger.

19,00 kr.

ISBN-10 1-9774-0522-3
ISBN-13 978-1-9774-0522-7
51900
9 781977 405227

www.rand.org

RR-3226-RC